1 Preface

The *open*FT product range transfers and manages files

– automatically,
– securely, and
– cost-effectively.

The reliable and user-friendly transfer of files is an important function in a high-performance computer network. Most corporate topologies today consist of networked PC workstations, which are additionally linked to a mainframe or Unix server. This allows much of the processing power to be provided directly at the workstation, while file transfer moves the data to the mainframe for further processing there as required. In such landscapes, the locations of the individual systems may be quite far apart. Fujitsu Siemens Computers offers an extensive range of file transfer products - the *open*FT product range - for the following system platforms:

- BS2000/OSD®
- Solaris™(SPARC®/Intel™), LINUX®, Reliant UNIX®, AIX®, HP-UX®, SCO Open Server®, OSF1(Tru64), UnixWare
- Microsoft® Windows 98/Me™, Windows NT™, Windows 2000™, Windows XP™, Windows Server 2003™
- OS/390 resp. z/OS (IBM®)

1.1 Brief description of the product

*open*FT for UNIX is the file transfer product for systems with the UNIX operating system.

All *open*FT products from Fujitsu Siemens Computers intercommunicate via *open*FT protocols (originally: FTNEA protocols), which were standardized by Siemens. Since a number of FT products from other software vendors also support these protocols, many interconnection options are available.

When used in combination with *open*FT-FTAM, *open*FT also supports the FTAM file transfer protocol (File Transfer Access and Management) standardized by ISO (International Organization for Standardization). This makes it possible to interconnect with even more systems from other vendors whose file transfer products support the same standard.

With the integrated FTAC function, *open*FT offers extended admission and access protection (FTAC stands for **F**ile **T**ransfer **A**ccess **C**ontrol).

1.2 Target group and objectives of this manual

This manual contains the information which is needed by *open*FT and FTAC administrators of UNIX systems for their work and which is not included in the User Guide.

For general information on file transfer and file management, you will also need the User Guide. Further literature is listed in the references.

The manual covers Reliant UNIX systems as well as portings to other UNIX platforms. The operating system-dependent differences are described in detail in the Release Notices supplied on the respective product CD. The examples refer to Reliant UNIX systems.

1.3 Concept of *open*FT for UNIX manuals

The complete description of *open*FT and its optional *open*FT-FTAM components comprises two manuals. In addition to this manual, there is also the user manual. The description is divided among the manuals as follows:

- *open*FT for UNIX - Installation and Administration

  The system administrator manual is intended for FT and FTAC administrators. It describes:
  - the installation of *open*FT and its optional components,
  - the operation, control and monitoring of the FT system and the FTAC environment,
  - the administration commands for FT and FTAC administrators and
  - important CMX commands.

- *open*FT for UNIX - Enterprise File Transfer in the Open World

  The user manual is intended for the *open*FT user and describes:
  - the basic functions of the *open*FT product family,
  - the conventions for file transfers to computers running different operating systems,
  - details on implementing FTAM,
  - the *open*FT user commands,
  - the BSFT interface,
  - the program interface and
  - the messages from the various components.

Many of the functions described in the manuals are also available in the *open*FT graphical interface. A detailed online help system that describes the operation of all the dialogs in the graphical interface is supplied together with the graphical interface. The online help system also contains a complete description of the *open*FT commands.

1.4 Changes since the last version of the manual

This section discusses the differences for the administrator between *open*FT for UNIX V8.1 and *open*FT for UNIX V8.0.

- Authentication

  *open*FT (Version 8.1 and later) for UNIX and Windows and V9.0 for BS2000 and z/OS supports an expanded addressing and authentication concept that provides secured, mutual identity checking of systems that are engaged in a transfer. It is based on the addressing of *open*FT instances, using network-wide, unique IDs and the exchange of partner-specific key information. This means that key pair sets can be created by the FT administrator for each local *open*FT instance. In turn, public keys of partner systems are stored in the directory *syskey* in the instance file tree of the local openFT instance. Administer local keys by using:

  – switch **-k** of the **fta** command to create a key pair set.

  – the new command **ftupdk** to update public key files.

  – the new switch **-dk=** of the **fta** command for deleting key pair sets.

  For defining the local instance ID, there is the new switch **-id=** in the **fta** command. Instance IDs of partner systems are used as file names for authenticating the public key files of the partner system. In addition, the instance IDs of the partner system should correspond to the address resolution using openFT, or using a TNS input if necessary.

- Expanding the *open*FT instance command

  In *open*FT version 8.0, previously created *open*FT instances can be updated for version 8.1 using the new command **ftupdi**. The current, existing instances are automatically updated during an update installation.
  ftcrei now checks the version of the instance directory to be switched on.
  ftdeli now checks whether the instance to be deactivated is the currently set instance or the standard instance.
  Using **ftshwi**, the path of the instance directory can be output using the new switch **-d**.

- Data integrity of the transferred data

  Using the new switch **-di** of the **ft** and **ncopy** commands, an integrity check of the transferred data can be explicitly requested using FT partners (Version V8.1 and later).

- New security levels in the admissions set.

  In connection with authentication, a new, more stringent security level 10 is introduced for partner systems that are authenticated in the local system. The previous security level 1 for partners, whose names are resolved via TNS, DNS, or /etc/hosts, has been moved to security level 90. *Open*FT automatically makes this change during an update installation.

- Additional logging outputs.

  FT log records of requests made using *open*FT partners now also contain specifications on the security functions used during the transfer.

- New request status conditions
  In connection with the new features *authentication* and *data integrity,* there are some new request status conditions, which can arise when the commands **fti -q** or **fti -l** are issued.

- Other modifications
  – A greater value for the maximum sentence length for text and binary files (32767).
  – A greater value for the maximum block length for text and binary files (65535).
  – Encryption can be disabled by setting the key length to 0.

1.5 Notational conventions

The following notational conventions are used throughout this manual:

`typewriter font`
: typewriter font is used to identify entries and examples.

italics
: In running text, names, variables and values are indicated by italic letters, e.g. file names, instance names, menus, commands and command options.

: indicates notes

Additional conventions are used for the command descriptions, see page 80.

1.6 README files

Information on any functional changes and additions to the current product version can be found in product-specific README files.

You will find the README files on your system under the directory */usr/readme/productname* or */opt/readme/productname*, provided you have installed them. You can view these files using an editor or print them out on a standard printer.

1.7 Current information on the Internet

Current information on the *open*FT family of products can be found on the World Wide Web under *http://www.fujitsu-siemens.com/openft*.

2 Tasks of the administrator

This chapter describes the most important administration tasks to be performed when running *open*FT. You can administer *open*FT both via the graphical interface (i.e. the desktop) and by using commands. The following options are available:

– Functions and commands that only the administrator may use (e.g. start *open*FT or delete log records),

– Functions and commands that are accessible to both the user and the administrator, but where the administrator is allowed to do more than the user (e.g. modify admission sets).

The tasks of the administrator include:

– Setting operating parameters[1) 2)]
– Starting and stopping *open*FT[1) 2)]
– Administering the request queue[1)]
– Viewing and deleting log records[1)]
– Administering admission sets and FT profiles[1)]
– Diagnostic options, e.g. switching the trace for error diagnostics on and off[1) 2)]
– Creating and administering instances in order to use *open*FT in the cluster
– Creating key pair sets [1)] and making a current public key available to the partner systems. This enables the local system to be authenticated by the partner.
– Obtaining the public keys of partner systems and suitably storing them in the local system so that the partner systems can be authenticated by the local system.

The administration functions marked with [1)] can also be executed via the ´graphical interface (i.e., the desktop), provided an X terminal or corresponding emulation is available. More information on the graphical interface can be found in the manual "*open*FT V8.1 for UNIX - User Guide" and in the online help installed with the graphical interface.

The administration functions marked with [2)] can also be performed via an SNMP management station.

Who is the *open*FT administrator?

*open*FT can only be administered under the login name *root*.

Who is the FTAC administrator?

The FTAC administrator manages admission sets and admission profiles. Both the *open*FT administrator and the FTAC administrator can manage logging.

Following a new installation, the *open*FT and FTAC administrators are identical (*root*). The FTAC administrator is identified by the fact that only his or her admission set is privileged. You can transfer this property to another login name by using the *ftmoda* command. This is useful, for example, if someone other than the system administrator is responsible for data security.

Depending on how (i.e., under which login name) the FTAC administrator has been set up, he or she will have different privileges and options, as explained below:

- Retention of *root* as the FTAC administrator or transfer of these privileges to another login name with *root* authorization:
  Every other login name (or user ID) with *root* authorization (i.e. UID=0) is also an FTAC administrator. Furthermore, the FTAC administrator has extended privileges (see the sections “FT profiles” on page 16 and “Saving the FTAC environment” on page 18).
- Transfer to a login name (or user ID) without *root* authorization (UID not equal to 0):
  The *open*FT administrator may no longer manage any admission sets and admission profiles. The FTAC administrator does not have extended privileges.
- Both the *open*FT administrator and the FTAC administrator can manage logging.

2.1 Operating parameters

The following parameters are available for controlling the operation of *open*FT. You can specify these parameters by means of the *fta* command:

- The instance identification of the local *open*FT instance.
- The maximum number of asynchronous requests that *open*FT should process simultaneously. You may specify maximum values separately for inbound requests (MAXISP) and outbound requests (MAXOSP).
- The upper limit for the length of blocks to be transferred.

  Following the installation of *open*FT/*open*FT-FTAM, the maximum block length is set to 65535 characters. This maximum length is not permissible for station links. Consequently, you must set the length to 3072 in this case.
- The scope for protocols during *open*FT operation.
- The variant of the code table that is to be used for requests to *open*FT partners.
- The length of the RSA key to be used for encryption purposes.

You can view the current values of the parameters for *open*FT with the *fti* command.

You can also view and change the current operating parameters via the graphical interface. To do this, open the *Operating Parameters* window by selecting the appropriate menu item in the *Administration* menu. You will find a detailed description of each function in the online help for the graphical interface.

Tips for performance control

When specifying the values for MAXISP / MAXOSP, you must consider the following points:

- Lower values mean that fewer FT requests can be run concurrently, but also implies that the performance of other applications will not be noticeably degraded on your processor.
- High values mean that a high volume of FT requests can be processed within a short period of time, but that the performance of other applications will be degraded on your processor.
- Different values for MAXISP / MAXOSP: if *open*FT is used on a server, it is useful is select a significantly higher value for MAXISP than for MAXOSP.

2.2 Starting and stopping *open*FT

By default, *open*FT is started automatically at system startup.

When *open*FT is stopped, only synchronous requests are executed. Asynchronous requests are stored in the request queue. So long as *open*FT is not started, no further requests are accepted from partner systems.

After being started, *open*FT executes both asynchronously issued requests as well as file transfer requests issued on the remote system.

You can start and stop *open*FT via the graphical interface (i.e. the desktop) with the the *Administration/Start asynchronous server* or *Administration/End asynchronous server* functions or via the *fta* command.

2.3 Switching the language interface

The language is not queried during installation. Instead, the *LANG* environment variable of the administrator installing *open*FT is evaluated and set as the default language. This value can be changed as follows:

- The *open*FT administrator can change the default setting with the *ftlang* tool. Only the setting specified via the *ftlang* tool is relevant for the output of the man pages.
- Each user can change his or her own language setting using the *OPENFTLANG* environment variable. The user must enter the first two letters of the language setting in the *LANG* variable (*de* or *en*) and then export the environment variable.

  Example

  `OPENFTLANG=de; export OPENFTLANG` corresponds to (for example): `LANG=De_DE.88591,De_DE.646,`etc.

  or

  `OPENFTLANG=en; export OPENFTLANG` corresponds to (for example): `LANG=En_US.ASCII,En_US.88591,`etc.

The following table shows the effects of setting (or not setting) the OPENFTLANG and LANG variables:

OPENFTLANG	**LANG**	**Result**
Not set or empty	Not set or empty	Default setting
Not set or empty	Invalid value	Default setting
Not set or empty	Valid language	Language set in LANG
Invalid value or a language that is not installed	Not evaluated	Default setting
Valid value (2 letters, both lower case, of an installed language)	Not evaluated	Language set in OPENFTLANG

2.4 Request queue

The request queue stores all asynchronous outbound requests, and all inbound requests. As the administrator, you can

- **obtain information** about all asynchronous requests on your system that are not yet completed. This includes the right to query information about all requests of all users. You can display the request queue with the *fti* command.
- **modify** the **processing order** of all requests on your system, including those of other users. You can do this by using the *ftmodr* command.
- **cancel** asynchronous requests on your system, including those of other users. You can do this by using the *ftc* command. In special cases, you must use the *ftrs* command.

You can also view the request queue in the graphical interface by clicking on the *Request Queue* object window. In addition, you can also execute the following functions via the graphical interface:
– Cancellation of asynchronous requests
– Clear the request queue
– Update the request queue
– Change the priority of requests

You will find detailed descriptions of the functions in the online help system of the graphical interface.

2.5 Log records

As an *open*FT or FTAC administrator, you may display and delete the log records of all users.

2.5.1 Displaying log records

You can use the *ftshwl* command to view all log records in the system. The output of a log record contains an RC column which indicates the cause of rejection or abort of the request by means of a 4-digit reason code. This column can also contain a positive acknowledgment to a request (reason code 0000). You can use the *fthelp* command to determine the meaning of the reason codes.

2.5.2 Deleting log records

FT and FTAC log records may be deleted by the *open*FT administrator and the FTAC administrator. To do this, use the *ftdell* command.

Basically, *open*FT writes an indefinite number of log records. However, if no more storage space is available on disk, FT requests are rejected. If you need continuous documentation over an extended period, you should therefore back up the existing records from time to time (e.g. by redirecting the output of *ftshwl* to a printer or to disk) and then remove these log records from the current log file. The benefit of this is, first, that the log records provide a complete documentation which can be maintained over long periods, and second, that the log file does not become unnecessarily large, thus resulting in slower access performance.

Deleting log records causes the size of the log file to change since the storage space is immediately free upon deletion. On starting up the operating system, all log records older than 30 days are deleted by default.

You can also view log records in the graphical interface by clicking on the *Logging* object window. You can also execute the following functions via the graphical interface:
– Delete log records
– Select log records
– Update log window

You will find a detailed description of each of the functions in the online help system of the graphical interface.

2.6 Admission sets

As the FTAC administrator, you specify the standard admission set and can view, modify and delete the standard admission sets for all users in the system.

2.6.1 Standard admission set

The standard admission set applies to all login names. The user can restrict this admission set further.

The user can override the entries in the standard admission set only,
– if you, as FTAC administrator, modify the admission set of the user accordingly,
– or if you set up a privileged FT profile.

Following installation of *open*FT, the standard admission set is set so that file transfer is possible without restriction. As FTAC administrator, you should therefore adapt the standard admission set to the protection requirements on your processor.

2.6.2 Displaying and modifying admission sets

Admission sets can be viewed using the *ftshwa* command. The entries made by the FTAC administrator are listed under MAX-ADM-LEVELS, the user entries under MAX-USER-LEVELS. The smaller value is valid in each case.

You can also view admission sets in the graphical interface by clicking on the *Admission Sets* object window. You will find a detailed description of each of the functions in the online help system of the graphical interface.

The settings in the admission set apply to all users initially. As the FTAC administrator, you can assign an individual admission set for each user in the system or modify an existing one. The *ftmoda* command is available for this purpose.

2.6.3 Using admission sets properly

To protect your processor against serious attempted intrusion, you should set the inbound properties in the admission set as restrictively as possible for the login name *root*, i.e. at least prohibit inbound processing.

1. For secure operation, you should prevent all inbound admissions in the standard admission set, e.g. by using the command:

   ```
   ftmoda @s -os=100 -or=100 -is=0 -ir=0 -if=0 -ip=0
   ```

2. For each user authorized to carry out inbound processing, you, as FTAC administrator, should set all parameters of the corresponding admission set to 100.

3. Recommend all users to change their inbound values to 0. They may then use their profiles and the “ignore ... level” function to permit any desired access mode. File transfers will then be allowed only via the FTAC transfer admission, but no longer via the login and password.

In version 8.1and later, it is possible for *open*FT partner to undergo a reliable identity check using cryptographic means (see the section “Authentication” on page 25). Using the value 10 in the admissions set, you can release basic functions to only those partner systems that are authenticated in the local system. In *open*FT version 8.1, the meanings of the numbers in the admission set were also modified. Whereas in older versions a **“1”** meant that the basic function could be used by all the partners in the TNS, this is now represented by the value **“90”** in version 8.1 and later.

The use of a file name prefix in the FT profile provides additional security. This prevents switching to a parent directory.

Important

If you have high security requirements, these actions are really only useful if *open*FT is the only active application for file transfer tasks on your processor, i.e. TCP/IP services like ftp, tftp must not be active!

2.7 FT profiles

As the FTAC administrator, you can create FT profiles for any user in the system and modify them later. The FTAC administrator is the only person who can assign privileges to FT profiles.

2.7.1 Creating FT profiles

You can create FT profiles with the command *ftcrep*. If you also want to assign a transfer admission at the same time, you must either have *root* authorization as the FTAC administrator or specify the password for the particular login name. If you do not have *root* authorization or specify the password, the profile is created without a transfer admission; the user must then assign it later.

When you create the profile, you can also assign privileges.

You can also create admission profiles in the graphical interface by opening the *Admission Profiles* dialog window via the *File/New* menu item. You will find a detailed description of each of the functions in the online help system of the graphical interface.

2.7.2 Viewing and modifying FT profiles

You can use the *ftshwp* command to display the FT profiles of all users. The transfer admission of the profile is not output, i.e. your administrator privileges do not grant you access to files on remote systems.

You can also view the admission profiles in the graphical interface by clicking on the *Admission Profiles* object window. You can also change admission profiles in the *Admission Profiles* dialog window. You will find a detailed description of each of the functions in the online help system of the graphical interface.

You can use the *ftmodp* command to make the following changes to an FT profile:

– assign or cancel privileges
– modify the transfer admission, if you have *root* authorization or know the password
– assign the profile to another login name

Following a modification of this nature, the profile will be locked, unless the FTAC administrator *root* has authorization (UID=0), and must be explicitly unlocked, e.g. by using the command *ftmodp ... -v=y*.

If a transfer admission is assigned for a second time, the existing transfer admission is locked.

2.7.3 Deleting FT profiles

You can use the *ftdelp* command to delete FT profiles of a user. This function is necessary, for example, after deletion of a login name, since the profiles are not automatically deleted when a login name is deleted. You should contact the user before you delete profiles from active login names.

You can also delete admission profiles via the graphical interface by selecting the *Delete* command from the context menu. You will find a detailed description of the object windows in the online help system of the graphical interface.

2.7.4 Assigning privileges to FT profiles

A privileged FT profile is intended for exceptional circumstances in which it is necessary for a user to override all restrictions. To assign privileges to a profile, you can use the command *ftmodp ... -priv=y*, for example.

Once a profile has been assigned privileges, it is possible only to modify the transfer admission and cancel the privileges. To prevent abuse, no other changes are permitted.

You can also assign privileges to admission profiles via the graphical interface in the *Admission Profiles* dialog window. You will find a detailed description of each of the functions in the online help system of the graphical interface.

2.8 Saving the FTAC environment

When migrating individual users to another processor, or when migrating the complete processor, it is possible to provide the users with the same FTAC environment by saving the admission sets and FT profiles and restoring them on the new processor. Furthermore, you can also created backup copies of the FTAC environment on your processor by this method.

2.8.1 Saving admission sets and FT profiles

You can use the *ftexpe* command for backups. You can select the admission sets and FT profiles which you wish to save for particular users. You must specify the name of the backup file.

In all cases, the standard admission set is not included in the backup. Instead, all the values of an admission set that refer to the standard admission set (represented by an asterisk (*) in the display) are stored as variables. This means that when they are restored, they will receive the value of the standard admission set valid at the time.

You can also save admission sets and admission profiles via the graphical interface using the *Export FTAC Environment* command in the *Administration* menu. You will find a detailed description of each of the functions in the online help system of the graphical interface.

Displaying saved admission sets and FT profiles

You can display saved admission sets and FT profiles with the *ftshwe* command. You must specify the name of the backup file.

You can also view saved admission sets and admission profiles via the graphical interface by dragging the export file into the *Exported Admissions* directory and then dropping it there.

2.8.2 Importing saved admission sets and FT profiles

You can re-import saved admission sets and FT profiles with the *ftimpe* command. Here, you must make a distinction between sets, profiles and login names, i.e. you must not accept the entire backup contents. Please note that the values which refer to the standard admission set are always assigned the values of the currently valid admission set.

If you have *root* authorization as the FTAC administrator, the admission profiles that you import will be immediately available with the status that was set on exporting the profile. If you do not have *root* authorization, imported profiles will initially remain locked for the login names (or user IDs) of other users.

You can also import admission sets and admission profiles via the graphical interface using the *Import FTAC Environment* command in the *Administration* menu. You will find a detailed description of each of the functions in the online help system of the graphical interface.

2.9 Setting the protection bit for newly created files

You can set the protection bit value for new files created for inbound requests to a value that greatly restricts the file access rights for the group and for other users.

You may modify the standard protection bit setting with the *umask* command. To ensure that the protection bit value is properly set when *open*FT is started, you should activate the command line *umask 027* in the startup file for the standard instance *std*. This startup file is located under */var/openFT/std/etcinit/openFTinst*.

If *umask 027* is not sufficient, then you can also activate *umask 0177* in the startup file. *umask 0177* means *rw* access for the owner only. To do this, remove comment character # at the beginning of the appropriate lines. All receive files created thereafter will then be assigned the access rights *-rw-------*.

If you start *open*FT manually, you must specify the protection bit setting according to your requirements before you start it.

2.10 AES encryption method

When connecting to *open*FT partners that support the AES algorithm (from version 8.0 onwards), the new RSA/AES encryption algorithm is used instead of the old RSA/DES algorithm for the request description data and user data.

A key pair set must exist in the local system so that you can transfer *open*FT request description data and file content in encrypted form (see page 27).

2.11 Diagnosis

To support error diagnostics, you can switch a trace on or off, prepare protocol files and output diagnostic information. These functions are primarily intended for the Maintenance and Diagnostic Service of the Fujitsu Siemens Computers GmbH.

Switching on and off trace mode

You can switch the trance mode on or off with the FT command *fta* or via the graphical interface. When the trace mode is enabled, the diagnostic data is written to trace files, which must be edited for further diagnostics.

Preparing log files

The trace files are located in the directory */var/openFT/instance/traces* where *instance* is the name of the corresponding instance. These files must be edited with the *fttrace* or *step* commands.

To create a trace log file You can switch the trace function on and off in the graphical interface in the *Operating Parameters* dialog window in the *Administration* menu. The trace log file can be displayed using the *Open Trace File* command in the *Administration* menu. You will find a detailed description of each of the functions in the online help system of the graphical interface.

Displaying diagnostic information

Unlike trace files, diagnostic records are written only if an error occurs. You can output these diagnostic records with the *ftshwd* command.

Message file for console commands:

In order to use the diagnostic trace information in console output, the output is also stored in the file */var/openFT/instance/log/conslog*, where *instance* is the name of the corresponding instance.

2.12 Using *open*FT in a cluster

From *open*FT version 8.0 onwards, you can run several *open*FT instances at the same time on a single host. These instances allow you to switch to a different computer already running *open*FT so that you can continue to use the *open*FT functionality when the initial host fails. You will find examples on how to use *open*FT in a UNIX cluster in the appendix.

A requirement for this is that *open*FT uses only the TCP/IP transport system. Other transport systems are not supported in a cluster and must also not be configured in the TNS. In a cluster, the same version of *open*FT must be running on all the computers.

For systems that do not have TCP/IP there is currently only the standard instance.

*Open*FT commands that call preprocessing, postprocessing or follow-up processing run in the same instance as the request that initiated the pre-, post- or follow-up processing.

If you administer *open*FT via SNMP, then please note when switching to the cluster that SNMP can only work together with one instance.
The decisive factor is which instance is set when the agent is started (see also chapter “Administering openFT via SNMP” on page 71).

Command for administering instances

As an *open*FT administrator you can create, modify and delete instances. You can also set up instances and obtain information on instances (like a user).

- Creating or activating an instance

  Using the command *ftcrei,* you can create a new instance or re-activate (switch on) a deactivated instance.

  When an instance is created, the operating parameters, the profile files, the startup and shutdown files are initialized as during a new installation.

  When an existing instance is deactivated, the existing instance file tree, with the operational resources of the instance, is linked to the directory */var/openFT*.

- Modifying an instance

  You can assign a different Internet host name to an instance with the *ftmodi* command.

- Deleting an instance

  You can delete an instance with the *ftdeli* command. Deleting an instance in this manner only removes the symbolic link in the local */var/openFT* directory. The instance file tree is not changed.

- Setting up an instance

  You can select the *open*FT instance you want to work with using the *ftseti* command.

  The command sets the OPENFTINSTANCE environment variable to the name of the instance.

  You can also set up the instance via the graphical interface. If there is more than one instance, then a list appears in the graphical interface from which you select the instance.

- Outputting information on instances

  You can query information on the instances using the *ftshwi* command.

- Updating an instance file tree

  Using the *ftupdi* command, you can modify the instance file tree of an older version of *open*FT for use in the current version. That is only necessary for instances that were not active at the time of an update installation.

– If you work with more than one instance, then in this case a separate *ftalarm* call is required for each instance (see also section “ftalarm - Report failed requests” on page 92).

– You will find detailed descriptions of the *ftcrei*, *ftmodi*, *ftupdi* and *ftdeli* commands in chapter “openFT commands for the administrator” starting on page 77. The *ftseti* and *ftshwi* commands are described in the “*open*FT for UNIX” User Guide.

Startup and shutdown file

In *open*FT version 8.1, there is one global startup and shutdown file that operates on all instances. In addition, every instance present also has its own startup and shutdown file.

During a system startup / shutdown, the global startup and shutdown file is called. This file then calls the startup and shutdown files of all *open*FT instances.

- Global startup and shutdown file:

  It is set up just like the previous startup and shutdown file under */etc/init.d* or in a corresponding directory on an external platform during the installation of *open*FT. This startup and shutdown file calls the startup and shutdown files of all instances when the system is started or when it is shut down.

- Startup and shutdown file specific to one instance:

  The startup and shutdown file *openFTinst* is created in the */var/openFT/std/etcinit* directory for the *std* instance during the installation of *open*FT.

  If you create another instance with *frcrei*, then a startup and shutdown file *openFTinst* is also set up for this instance in the directory */var/openFT/instance/etcinit* (*instance* = name of the new instance).

  The instance-specific startup and shutdown file matches for the most part the *open*FT V7.0 startup and shutdown file.

2.13 Authentication

If data requiring an extremely high degree of security is to be transferred, it is important that the respective partner system undergo a reliable identity check (“authentication”) before the transfer. The two *open*FT instances that are engaged in a transfer must be able to mutually check each other using cryptographic means, to ensure that they are connected to the “correct” partner instance.

In versions of *open*FT after version 8.1, for UNIX and Windows or version 9.0 for BS2000 and z/OS, an expanded addressing and authentication concept is supported. This is based on the addressing of the *open*FT instances, using a network-wide, unique ID, and the exchange of partner-specific key information.

When communicating with partners that are still using *open*FT version 8.0 (or older), the functions described in the following are not yet usable. The previous addressing concept is still supported for these partners for the sake of compatibility. In FTAM partners, authentication is not available in this form, since the FTAM protocol standardized by the ISO does not provide for comparable functionality.

2.13.1 Instance Identifications

Each *open*FT instance that works with authentication, must be assigned a network-wide, unique instance identification (instance ID). This also applies to *open*FT systems that only work with the standard instance (for example, on transport protocols other than TCP/IP). The instance ID replaces the previous addressing of *open*FT instances using processor and application names. The instance ID is a unique name up to 64 characters long, which must not be case-sensitive. An instance ID may consist of alphanumeric characters or the special characters “.”, “-” or “%” and may have a maximum length of up to 64 characters. The first character must be alphanumeric or be the special character “%”. The character “%” can only be used as an initial character. An alphanumeric character must follow a “.”.

In order to ensure the network-wide, uniqueness of the instance ID, you should proceed as follows when allocating the instance IDs:

- If the *open*FT instance has a network address with a **DNS name** you should use this as the ID. You can create an “artificial” DNS name for an openFT instance, by placing another part of a name in front of an existing “neighboring” DNS name, separated by a period.

- If the *open*FT instance does not have a DNS name, but is connected to a TCP/IP network, you should use the ID **%ip***n.n.n.n*, (where *n.n.n.n* is the IP address of the local *open*FT instance without the leading zeros in the address components).
- If the *open*FT is connected to an ISDN network and not to a TCP/IP network, you should use the ID **%isdn***mmmmmmmm* (where *mmmmmmmm* is the ISDN call number, including the country and local prefix).
- If the *open*FT is connected to an X.25 network (but not to either a TCP/IP or an ISDN network), the ID should begin with **%x25** and should contain the X.25 number and, where necessary, the NSAP; it should look like this **%x25***mmmmmmmmmmNSAP*.

You currently allocate these IDs for your local *open*FT instances with the parameter *-id=* of the *fta* command.

You should not explicitly use the form of instance ID (%.*processor*.*entity*), which is used internally by *open*FT for partners with a version earlier than version 8.1.

Instance IDs of partner systems should, from your local system's point of view, correspond to the partner name, by which the partner system is known in the *open*FT. This can be done either implicitly (name resolution via DNS/NIS, entry in the */etc/hosts*) or explicitly, by an entry in the TNS. The global name must then correspond to the instance ID of the partner. With the aid of the instance IDs of the partner systems, *open*FT administers operational resources like, for example, request waiting queues and cryptographic keys.

2.13.2 Creating and administering local keys

A suitable, public key for the given instance must be made available to the partner system, so that your own *open*FT instance can be authenticated in the partner system. Using *fta -k* (or by using the graphical user interface), create RSA key pairs for the local *open*FT instance that currently consist of a private key and a public key. A key pair set in UNIX currently consists of a key pair with a length of 768 and 1024 bits. Private keys are internally administered by *open*FT, public keys are stored in the *config* directory of the instance file tree of the *open*FT instance (Standard: */var/openFT/std/config)* under the name **syspkf.r<key reference>.l<key length>**. The key reference is a numerical designator for the version of the key pair. The public key files are text files that are created using the character code of the respective operating system, i.e. EBCDIC.DF04-1 for BS2000 and z/OS, ISO8859-1 for UNIX and Windows.

In the *syspkf.comment* file in the *config* directory of the instance file tree, you can store comments, which are written in the first lines of the public key files when a key pair set is created. The *syspkf.comment* is a text file that you can edit. The comments could, for example, contain the contact information of the FT administrator on duty, the computer name, or similar information that is important for partners. The lines in the file *syspkf.comment* can only be a maximum of 78 characters long. Using the command *ftupdk,* you can also import subsequent comments from this file into existing public key files.

If a public key file were accidentally deleted, you could re-create the public key files of the existing key pair set using *ftupdk*.

If you want to replace a key pair set with a completely new one, you can create a new key pair set using *fta -k.* You will recognize the most up-to-date, public key by the highest value key reference in the file name. *open*FT supports a maximum of three key pair sets at a time. The existence of several keys, however, should be temporary, until you have made the most up-to-date public key available to all partner systems. Thereafter, you can delete key pair sets that are no longer needed using *fta -dk=*. Deleted key pair sets can not be restored using *ftupdk*.

2.13.3 Distributing the keys to partner systems

Distribution of public key files to your partner systems should take place using reliable means, for example by

- distributing them via cryptographically secure by e-mail
- distributing them on a CD (by courier or by registered mail).
- distributing them via a central, *open*FT file server, whose public key is in the partners' possession.

If you want to transmit your public key files to partner systems using BS2000 or z/OS or OS/390, you must ensure that these files are re-coded from ISO 8859-1 to EBCDIC.DF04-1 (e.g. by transferring them as text files via *open*FT).

The public key file of your local *open*FT instance is stored in the partner system in the following location:

- For partners using *open*FT for BS2000 as type D, PLAM elements in the library **SYSKEY** on the configuration user ID of the partner instance. The partner name allocated to your openFT instance in the remote network description file must be selected as the element name.
- For partners using *open*FT for UNIX in the directory **/var/openFT/*instance*/syskey**. The instance ID of your local openFT instance must be selected as the file name. The file name must not contain any uppercase characters. If the instance ID contains any uppercase characters, they must be converted to lowercase characters in the file name.
- For partners using *open*FT for Windows in the directory **openFT\var*instance*\syskey**. The instance ID of your local openFT instance must be selected as the file name.
- For partners using *open*FT for z/OS or OS/390 as a PO element in the library ***admuser*.SYSKEY.** The partner name allocated to your openFT instance in the remote network description file must be selected as the element name.

2.13.4 Administering the keys of partner systems

The public keys of the partner systems are stored in UNIX as files in the directory *syskey* of the instance file tree of the local *open*FT instance (Standard: */var/openFT/std/syskey*). The instance ID of the partner system must be selected as the file name. The file name must not contain any uppercase characters. If the ID contains any uppercase characters, they must be converted to lowercase characters. If an updated, public key is made available by the partner instance, the old key file must be overwritten at that time.

2.13.5 Local and partner authentication

Basically, there are three distinct usages:

- The local *open*FT instance checks the identity of the partner instance. This assumes that a current, public key of the partner instance was stored locally in the *syskey* directory, the name of which corresponds to the instance ID of the partner instance. A configuration of this kind makes sense, for example, if a file server's files are to be accessed via openFT. It is important for the local *open*FT instance, that the received data come from a reliable source (the authenticated partner), in turn, it is not important to the file server, who is accessing it there.
- The partner instance checks the identity of the local *open*FT instance. This requires that a current, public key of the local *open*FT instance is stored in the partner instance (re-coded for BS2000- and z/OS- or OS/390 partners). A configuration of this kind would be conceivable, for example, if partner systems in several branch offices were to be accessed from a central computer via *open*FT and the branch computers were only permitted to access the central computer (and, in fact, only the central computer).
- The two *open*FT instances engaged in a transfer authenticate each other. This requires that current, public keys were mutually exchanged and the partners address each other via their instance IDs. In this way, it can be guaranteed that the data both came from a reliable source, and will also only end up in reliable hands.

3 Installation and configuration

This chapter describes the installation and configuration of *open*FT. In particular, it includes details of the TS applications required for the operation of *open*FT.

3.1 Installation of *open*FT

The installation of *open*FT is performed under the login name *root*.

The installation technique of *open*FT depends on the operating system and is described in the respective Release Notice. There are three different types of installation depending on if an FT version is already installed or which FT version is already installed on your computer:

- Initial or full installation
  This means that your computer does not have any FT version on it or that your current version needed to be deleted beforehand as was the case for *open*FT version 7.0 (or earlier), for example.
- Update installation
  This means that your computer has *open*FT version 8.0 installed.
- Installation of a correction version
  This means that your computer has *open*FT version 8.1 installed.

What you need to observe before installing *open*FT ...

- If CMX or PCMX has not yet been installed, you will need to first install PCMX (for Reliant UNIX or UnixWare) or CMX (for all other platforms) from the supplied storage medium before installing *open*FT. Make sure after installing CMX that the *tnsxd* and *cmxredd* processes are running. They must be running before you install *open*FT.
- If you want to install *open*FT-FTAM on a system in which the *open*FT installation takes place in a dialog, then you need to answer a question asking you if you have a valid *open*FT-FTAM license with *yes*.

  This question is not asked on HP, AIX and Linux systems. *open*FT-FTAM is only installed automatically with *open*FT if the installation is an update or a patch and if the FTAM functionality was already present. In all other cases you must install *open*FT-FTAM afterwards using the *install.ftam* command. You will find *install.ftam* in the directory */opt/openFT/bin/ftbin*.

- The language used in *open*FT (German, English) is not queried anymore during the installation. The language is now selected using the *LANG* environment variable. For this reason, the response file only contains the *FTAM* variable and does not contain the *LANM* variable anymore (see also section “Switching the language interface” on page 11).
- If you want to encrypt user data, you must also install *open*FT-CR for UNIX. This software is offered without a license at a fixed price. If an openFT-CR version ≤ V7.0 iis already installed, then you must first uninstall this version before installing *open*FT, and then you can install *open*FT-CR V8.0 .

The following three sections describe which steps must be performed for the three installation variants by you as the system administrator as well as those which are handled automatically by the installation procedure.

3.1.1 Initial or full installation

If you have not installed *open*FT on your system yet, the installation is an initial installation.

If *open*FT version 7.0 (or earlier) is installed, then it is a full installation.

Tasks required of the system administrator

1. If *open*FT version 7.0 (or earlier) and possibly add-on products are already installed, then you should save admission profiles and admission sets that are still needed in an external file using *ftexpe*. After this, you must uninstall *open*FT and the add-on products.
2. You must install the *open*FT version 8.1 product software.
3. If you want to install *open*FT-FTAM on a system in which the *open*FT installation takes place in a dialog, then you need to answer a question asking you if you have a valid *open*FT-FTAM license. If answered with *yes*, then *open*FT-FTAM is installed, otherwise it is not installed.

   This question is not asked on HP, AIX and Linux systems. If you want to use the FTAM functionality on these systems, then you must activate *open*FT-FTAM via the *install.ftam* command after installing *open*FT (see also section “install.ftam - Install openFT-FTAM” on page 150).
4. Later, the saved admission sets and admission profiles can be re-introduced using ftimpe. All security levels in the admission sets that were previously set at 1 are automatically converted to 90. The standard admission set is re-set.

After these steps, *open*FT will be fully operational and will be activated at each system startup.

Steps performed automatically

During installation, the following steps are carried out automatically:

- For an initial installation, standard TNS entries are created for *open*FT; for a full installation, existing entries for *open*FT are modified (see the section “TNS entries created automatically” on page 45).
- The operating parameters (e.g. maximum number of inbound and outbound requests that can be processed simultaneously, maximum block length, scope of FT and FTAC logging, setting of the character set) are set to default values. The node name of the processor is entered as the processor name (corresponds to the output in *uname -n*). The DNS name of the computer (if

one exists) is pre-set as the instance ID for the standard instance. When there is no DNS name, the node name of the computer is used for the instance ID.

- The following startup and shutdown files are set up:
  - The startup and shutdown file that applies to all instances (e.g. */etc/init.d/openFT* under Solaris)
  - The startup and shutdown file for the *std* instance (path: */var/openFT/std/etcinit/openFTinst*).

  With the help of this file *open*FT is started automatically each time the system is started, and is terminated automatically each time the system is shut down (see also section “Using openFT in a cluster” on page 22).
- A standard admission set permitting all file transfer functions is created.
- A key pair set is created (see page 27).
- The file transfer is started (but not on HP systems).

3.1.2 Update installation from *open*FT V8.0

If *open*FT V8.0 is already installed, an update installation is performed.

The following points must be observed:

- Log files are no longer deleted. They are carried over into the new version.
- Existing requests are deleted from the request queue unconditionally. If any follow-up processing was specified with the option *-lf=* in the submitted request, this is completed in the process.
- Existing trace files, if any, and the *DIAGFILE* are deleted.

Tasks required of the system administrator

1. You must load the product software.
2. If you want to install *open*FT-FTAM on a system in which the *open*FT installation takes place in a dialog, then you need to answer a question asking you if you have a valid *open*FT-FTAM license. If answered with *yes*, then *open*FT-FTAM is installed, otherwise it is not installed.

   This question is not asked on HP, AIX and Linux systems. *open*FT-FTAM is automatically installed on theses systems if it was installed in *open*FT V8.0.

Steps performed automatically

The following steps are performed automatically for an update installation:

- Current fta processes and the graphical user interface are terminated.
- The TNS entries from the previous version are taken over.
- The language setting is carried over from the previous version.
- If you are working with HP, AIX, or Linux systems, *open*FT FTAM is automatically installed, if it was already installed in *open*FT version 8.0.
- The new instance-overlapping startup and shutdown file (e.g. */etc/init.d/openFT* on Solaris) is installed. The old instance-overlapping startup and shutdown file is no longer automatically saved.
- The instance directories of currently existing instances and of the standard instance are updated. During this, the following steps are carried out:
  – The operating parameters (e.g. maximum number of inbound and outbound requests that are being simultaneously processed, the maximum block lengths, the scope of the FT and FTAC logging, setting the charac-

ter set and processor name, etc.) are carried over from the previous version for all *open*FT instances. The DNS name of the computer (if one exists) is preset as the instance ID for the standard instance. When there is no DNS name, the node name of the computer is used for the instance ID (corresponding to the output from *uname -n*).
  - The old instance-specific startup and shutdown files */var/openFT/<instance>/etcinit/openFTinst* are stored to */var/openFT/<instance>/etcinit/openFTinst .old*. Subsequent to this, the new instance-specific startup and shutdown files are installed.
  - If you have made modifications in the old startup and shutdown files, you must also make them in the new start up and shutdown files, if applicable. See the section “Using openFT in a cluster” on page 22
  - The FTAM catalog is carried over from the previous version.
  - The log records are carried over from the previous version.
  - The admissions set and admissions profile are carried over from the previous version. All security levels that were previously set to 1 in the admissions sets are automatically converted to 90.
  - A key pair set is created (see page 27).
- Instance directories that were not switched on at the time of the update installation (i.e. directories from instances that were switched off in version 8.0 using *ftdeli*), are not updated. If they are to be used again, they must be updated using *ftupdi*.
- The file transfer is started for those instances, for which it was started before the installation (not applicable on HP systems).

3.1.3 Installation of a patch

Installation of a patch means that *open*FT V8.1 is already installed on your computer.

Tasks required of the system administrator

1. You must load the product software.
2. If you want to install *open*FT-FTAM on a system in which the *open*FT installation takes place in a dialog, then you need to answer a question asking you if you have a valid *open*FT-FTAM license. If answered with *yes*, then *open*FT-FTAM is installed, otherwise it is not installed.

   This question is not asked on HP, AIX and Linux systems. *open*FT-FTAM is automatically installed on theses systems if it was installed in the previous version.

Steps performed automatically

The following steps are performed automatically on installing a patch:

- Current *fta* processes and graphical user interfaces are terminated
- The FT profiles and admission sets, the log files, the startup and shutdown files, the FTAM catalog and the request queue (operating parameters and requests) and the key pair sets are taken over without changes for all *open*FT instances.
- If you work on an HP, AIX or Linux system, then *open*FT-FTAM is automatically installed on theses systems if it was installed in the previous version.
- The language setting from the previous version is used.
- The file transfer is started for those instances, for which it was started before the installation (not applicable on HP systems).

3.1.4 Activities after installation

Following the installation of *open*FT, you may need to perform additional steps, depending on what you require of your system. These may include the following:

- TNS entries
- encryption
- distributing public keys and obtaining public keys for partner systems needing to be authenticated.
- Identifying instances and specifying the name of the local system for *open*FT
- disabling automatic startup of *open*FT
- automatic saving of log records in files, followed by deletion
- activating *ftalarm* function
- maximum block length for station links
- starting *open*FT subagents automatically
- installing and uninstalling *open*FT-FTAM

TNS entries

Whether you have to make TNS entries, and if so, how they should look, is described in the section “Entering transport system applications” on page 44.

Please note that cluster configurations are only supported for TCP/IP. You will therefore need to check all *open*FT-specific TNS entries for cluster configurations and delete those transport system entries that are not related to TCP/IP. (i.e. everything but RFC1006 and LANINET).

Encryption

If you want to use encryption for user data in addition to request description data, you must install *open*FT-CR version 8.0 for UNIX.

When connecting to *open*FT partners that support the AES algorithm (e.g. *open*FT version 8.0 and later for UNIX and *open*FT V8.0 and later for BS2000/OSD), the request description data and user data are encrypted using the new RSA/AES algorithm (instead of with the previous RSA/DES algorithm).

So that you can transfer *open*FT request description data and file content in encrypted form, there must be a key pair set in the local system (see page 27). A key pair set is created during installation of *open*FT and consists of private and public keys of suitable length.

Other key pair sets can be created (if necessary) using *fta -k* . Obsolete key pair sets are deleted using *fta -dk=*.

Private keys are internally administered by *open*FT. Public keys are saved under the name **syspkf.r<key reference>.l<key length>** in the *config* directory of the instance file tree of the *open*FT instance (standard: */var/openFT/std/config*). The key reference is a numerical designator for the key pair version.

Distributing public keys and obtaining public keys for partner systems to be authenticated.

If your local system is to be authenticated in partner systems, then public keys for your system need to be made available to the partner systems. You can find details in the section “Distributing the keys to partner systems” on page 28.

If partner systems are to be authenticated by *open*FT, you will need the public keys of those partners. The public keys of the partner system are stored in UNIX as files in the directory *syskey* of the instance file tree of the local *open*FT instance (standard: */var/openFT/std/syskey*). The instance ID of the partner system must be selected as the file name. The data name must not contain any uppercase characters. If the ID contains uppercase characters, these must be converted to lowercase characters in the file name. If an updated public key is made available by the partner instance, the old key file must be overwritten.

Specifying the instance ID and the name of the local system for *open*FT

*open*FT sends a sender address along with the request to a remote system. This sender address must be known to *open*FT before you issue requests. Partner systems using *open*FT version 8.1 and later, are identified by the so-called “instance ID.” The local instance ID is defined using the command *fta -id=* (or by using the graphical user interface). You will find details on this in the section “Instance Identifications” on page 25.

For connecting to an older version of *open*FT on BS2000/OSD, OS/390 or z/OS, *open*FT needs a sender address. With a processor link, the node name of your processor is also sent as the sender address. The network administrator for your processor has stipulated the node name for your processor (*uname -n*). With installation of *open*FT, the node name is automatically entered as the processor name. In this case, you do not have to take any action.

With a station link, you must specify the node name of the upstream station as the processor name as well as the name of your station. To do this, use the *fta* command.

More details on the *fta* command and the *-id, -p* and *-l* options can be found in the description on the *fta* command starting on page 85.

Disabling the automatic startup of *open*FT

During installation, the startup file is installed (e.g. */etc/rc2.d/S73openFT* on Solaris), with which file transfer is automatically initiated at system startup. This script calls the file */var/openFT/std/etcinit/openFTinst* when the system starts, which then automatically starts the file transfer.

If *open*FT instances were created using the *ftcrei* command, then this script also calls the startup and shutdown file for this instance (see also section “Using openFT in a cluster” on page 22).

These files then start the file transfer for the corresponding instance.

If you do not want file transfer to be started automatically, you will need to comment out the corresponding command line in the file */var/openFT/std/etcinit/openFTinst* or in the startup and shutdown file for the instances.

Disabling the automatic termination of *open*FT

During installation, the shutdown file is installed (e.g. */etc/rc0.d/K27openFT* on Solaris.). This script calls the file */var/openFT/std/etcinit/openFTinst* when the system shuts down, which then automatically terminates the file transfer.

If *open*FT instances were created using the *ftcrei* command, then this script also calls the startup and shutdown file for this instance (see also section “Using openFT in a cluster” on page 22).

These files then terminate the file transfer for the corresponding instance.

If you do not want file transfer to be terminated automatically, you will need to comment out the corresponding command line in the file */var/openFT/std/etcinit/openFTinst* or in the startup and shutdown file for the instances.

Automatic saving of log records in files, followed by deletion

The logging file can grow exponentially and quickly fill the disk on which it is saved. It is therefore extremely important that this file be monitored and purged on a regular basis.

In order to keep the size of the logging file as small as possible, all log records older than 30 days are automatically deleted whenever the system is started. If you want to define some other time period, you will need to modify the corresponding line in the startup and shutdown file */var/openFT/std/etcinit/openFTinst* and/or in the startup and shutdown files of other instances.

If you also want all log records to be to be saved before being deleted, you can add an appropriate *ftshwl* command in the startup and shutdown file. An example of this is already included as a comment in the startup file.
You will find an example for the cyclical deletion of log records at *http://www.fujitsu-siemens.com/openft* under the item *Application Scenarios*.

Enabling the ftalarm command

If you want to be informed about the frequency of failed FT requests, it is advisable to use the *ftalarm* command for this purpose. If desired, you can also have the *ftalarm* command automatically started at system startup by inserting a corresponding line with the *ftalarm* command in the startup and shutdown file */var/openFT/std/etcinit/openFTinst* and/or in the startup and shutdown files of other instances.

Starting the *open*FT subagent automatically

If you want to automatically start the *open*FT subagent for administration using SNMP at system startup, you must activate the corresponding line with the *ftagt* command in the startup and shutdown file */var/openFT/std/etcinit/openFTinst* and/or in the startup and shutdown files of other instances.

More details on this can be found in the chapter “Administering openFT via SNMP” on page 71.

Please note for clusters that SNMP can only work with a single instance. The deciding factor is which instance is set up when the agent is started (see also section “Using openFT in a cluster” on page 22).

Installing and uninstalling *open*FT-FTAM

*open*FT-FTAM is not installed together with *open*FT when the installation is an initial or full installation on an HP, AIX or Linux system. The same applies to update or patch installations when *open*FT-FTAM was not installed beforehand.

In these cases you need to install *open*FT-FTAM using the *install.ftam* command after installing *open*FT (see also section “install.ftam - Install openFT-FTAM” on page 150).

Installation is only permitted when you also have a valid *open*FT-FTAM license available.

You can also uninstall *open*FT-FTAM if it is not needed anymore using *install.ftam*. *open*FT-FTAM must be uninstalled if you do not have the corresponding license.

3.1.5 Automatic installation

You may also select automatic installation when installing *open*FT on some systems such as Reliant UNIX. In this case, installation is carried out without user prompts on screen. The additional data for the desired language interface and the FTAM server required for installation of *open*FT are taken from the *response* file. For *open*FT, a standard response file is supplied. It has the following contents:

```
FTAM='NO'
```

Meaning of the environment variable

FTAM

specifies whether or not you are authorized to use the FTAM functionality, i.e. whether or not you have an *open*FT-FTAM license. In the standard response file, this variable is preset to *NO*, i.e. *open*FT-FTAM is not installed.

Other possible values:
YES, i.e. you are authorized to use the FTAM functionality, i.e. you have an *open*FT-FTAM license. *open*FT-FTAM is therefore installed. You are then able to use *open*FT-FTAM.

3.2 Entering transport system applications

In order to use the functions of *open*FT, the FT applications required must be made known to the Transport Name Service (TNS). The TNS identifies a transport system application (TS application) by means of a symbolic name known as the GLOBAL NAME. The symbolic name generally consists of up to five name parts.

These symbolic names are assigned address information. The necessary specifications, such as station name, application name, port number, etc. can be obtained from your network administrator.

Depending on the installation variant, (initial, full or update installation) and the type of link, the necessary mandatory entries are made or modified during the installation of *open*FT; see also the section “TNS entries created automatically” on page 45.

Otherwise, you must make the entries yourself. The entries in the TNS can be made with the aid of the TNS compilers *tnsxcom*. To do this, enter the TS applications in a file, and then translate this file with the aid of the TNS compilers *tnsxcom* (see the section “tnsxcom - Create the TS directory” on page 166).

If you have installed CMX, you may also enter partner applications via a menu. Note, however, that only the CMX GUI can be used for FTAM partner applications. For further details, refer to the CMX manual.

All local TS applications for *open*FT, as well as all remote TS applications for the partners systems which are to be accessible for requests issued locally must be entered in the case of an SNA link.

Exceptions

- Partner systems which are accessible via TCP/IP can also be reached via the TCP/IP host name or the Internet address, possibly supplemented with the special port number. In this case, a standard entry with the GLOBAL NAME *ftstd* is sufficient for all partner systems addressed in this way.
- Partner systems which are accessible via ISDN are also accessible via the ISDN numbers in an FT request. In this case, a standard entry with the GLOBAL NAME *ftstdisdn* is sufficient for all partner systems addressed in this way.

It can also be useful to enter the remote TS applications of the partner systems which are to issue requests to the local system. In *open*FT partner version 8.1 and later, ensure that the name, by which requests are processed with this partner, correspond to the instance ID of the remote system. If there is any doubt, a TNS input is required.

In this case, In the case of WAN partners, the partner is easier to identify for requests issued in the remote system. For example, the name of the partner as entered in the TNS is recorded in the log records. With FTAM partners, an entry in the TNS is the precondition for automatic restart.

Which entries are created or modified for which installation variant and which type of link are explained in the following section entitled “TNS entries created automatically”.

The procedure for the entry of local and remote TS applications is explained starting on page 49.

TNS entries for cluster configurations

Please note that cluster configurations are only supported for TCP/IP. You will therefore need to check all *open*FT-specific TNS entries for cluster configurations and delete those transport system entries that are not related to TCP/IP. (i.e. everything except for RFC1006 and LANINET). You will find an example of this in the appendix.

3.2.1 TNS entries created automatically

During the installation of *open*FT, depending on the installation variant, the FT applications required for FT operation are automatically entered in the TNS or the existing entries are modified.

It is generally advisable not to modify the applications entered during the installation. If this is required in any case, it must be ensured that the port number of the $FJAM entry is divisible by 100 and that the port number of the $FJAM_OUTBOUND entry is equal to the port number of the $FJAM entry + 1. If your system is protected by a firewall and is to be accessible from the outside, the $FJAM input port must be released in the firewall.

If you wish to set up links via STA1/MSV1 (STANEA) or TRANSIT-LU0 (EMSNA), you must enter the local TS applications for *open*FT yourself. Existing entries are not modified.

Initial installation

For an initial installation, the following TNS entries are made automatically (see also the file */opt/openFT/config/tnsstd*):

```
$FJAM\
   TSEL    WANNEA   T'$FJAM'    ; entry for WAN-NEA,WAN-NX25,
                                ; ISDN-NEA,ISDN-NX25
   TSEL    LANSBKA  T'$FJAM'    ; entry for ETHN-CLNS/passive
                                ; necessary with link to CMX V3.0
   TSEL    WANSBKA  T'$FJAM'    ; entry for WAN-CONS,
                                ; ISDN-CONS
   TSEL    OSITYPE  T'$FJAM'    ; entry for ETHN-CLNS/active
   TSEL    RFC1006  T'$FJAM'    ; entry for TCP/IP-RFC1006
   TSEL    LANINET  A'1100'     ; entry for TCP/IP

$FJAM_OUTBOUND\
   TSEL    WANNEA   T'$FJAMOUT' ; entry for WAN-NEA,WAN-NX25,
                                ; ISDN-NEA,ISDN-NX25
   TSEL    LANSBKA  T'$FJAMOUT' ; entry for ETHN-CLNS/passive
                                ; necessary with link to CMXV3.0
   TSEL    WANSBKA  T'$FJAMOUT' ; entry for WAN-CONS,
                                ; ISDN-CONS
   TSEL    OSITYPE  T'$FJAMOUT' ; entry for ETHN-CLNS/active
   TSEL    RFC1006  T'$FJAMOUT' ; entry for TCP/IP-RFC1006
   TSEL    LANINET  A'1101'     ; entry for TCP/IP

$FTAM
   PSEL    V''                  ; empty presentation selector
   SSEL    V''                  ; empty session selector
   TSEL    WANSBKA  T'$FTAM'    ; entry for WAN-CONS,ISDN-CONS
   TSEL    LANSBKA  T'$FTAM'    ; entry for ETHN-CLNS/passive
                                ; necessary with link to CMXV3.0
   TSEL    OSITYPE  T'$FTAM'    ; entry for ETHN-CLNS/active
   TSEL    RFC1006  T'$FTAM'    ; entry for TCP/IP-RFC1006
   TSEL    LANINET  A'4800'     ; entry for TCP/IP

ftstd\
   TA      RFC1006 255.255.255.254    PORT 1100 T'$FJAM'

ftstdisdn\
   TA      WANSBKA E.164   0    T'$FJAM'  2/2  WAN 1
```

The local TS application $FJAM is the contact for inbound requests from *open*FT partners, $FJAM_OUTBOUND for outbound requests to *open*FT partners. The $FJAM_OUTBOUND entry permits parallel processing of 200 outbound requests. This value can be restricted for asynchronous requests using the operating parameter *maxosp*, which is specified by the FT administrator with the *fta* command.

If you want set up links via TRANSIT-LU0 (EMSNA), you must remove the $FJAM_OUTBOUND entry and add the TSEL entries required for $FJAM. The TS applications for the outbound requests must be entered with $FJAM001, $FJAM002, ... (see the section “Definition of local TS applications for openFT for SNA links” on page 49).

The local TS application $FTAM is the contact for all inbound and outbound requests with FTAM partners.

ftstd is a standard entry for partner systems which are accessible via TCP/IP. They can thus be addressed via the TCP/IP host name or the Internet address, possibly supplemented with a port number.

ftstdisdn is standard entry for partner systems which are accessible via ISDN. They are thus accessible by directly inputting the ISDN number. The entry can The entry can vary depending your system configuration and need not be matched as a rule.

Full installation, update installation

With a full installation or an update installation from FT-SINIX V5.2, the existing TNS entries are modified as follows:

- If a $FJAM001 entry exists and does not contain a TSEL entry for an SNA link (EMSNA), the following takes place during installation:

  1. The TS application $FJAM001 is renamed to $FJAM_OUTBOUND. The $FJAM_OUTBOUND entry permits the parallel processing of 200 outbound requests with *open*FT partners. This value can be restricted for asynchronous requests using operating parameter *maxosp*, which the FT administrator can set with the *fta* command.
  2. The TS applications $FTJAM002 up to $FJAM016 are deleted.

- If a $FJAM001 entry exists and does contain a TSEL entry for an SNA link (EMSNA), no $FJAM_OUTBOUND entry is create during installation. The TS applications for the outbound requests must be entered with $FJAM001, $FJAM002, ... in the case of a station link or SNA link (see the section “Definition of local TS applications for openFT for SNA links” on page 49).
- If no $FJAM001 exists, a $FJAM_OUTBOUND entry is created.
- If no $FTAM entry exists, a standard entry is created for $FTAM. The local TS application $FTAM is the contact for all inbound and outbound requests with FTAM partners.

- If the *ftstd* entry is missing, a standard entry is created for *fstd*. *ftstd* is a standard entry for all partner systems which are accessible via TCP/IP and which can thus be addressed via the TCP/IP host name or the Internet address, possibly supplemented with a port number.
- If the *ftstdisdn* entry is missing, a standard entry is created for *ftstdisdn*. *ftstdisdn* is a standard entry for all *open*FT partner systems which are accessible via ISDN. They are thus accessible by directly inputting the ISDN number. They are thus accessible by directly inputting the ISDN number. The entry can The entry can vary depending your system configuration and need not be matched as a rule.

3.2.2 Definition of local TS applications for *open*FT for SNA links

If you wish to set up links via STA1/MSV1 (STANEA) or TRANSIT-LU0 (EMSNA), then the entry $FJAM_OUTBOUND must not be present. In this case, you must enter the local TS applications for *open*FT yourself.

The entries are made in the menu system or in the file which is translated using the TNS compiler *tnsxcom*. *open*FT applications do not require NEA migration functions.

For *open*FT, the local TS application must be entered with the symbolic names (GLOBALEN NAMEN) $FJAM and $FJAM0*nn* (01 ≤ nn ≤ 99). The application $FJAM is the contact for inbound requests from remote *open*FT partners; the $FJAM0nn applications process the outbound requests to *open*FT partners in the case of station and SNA links. *nn* must be assigned in only in ascending order without gaps, starting at $FJAM001 ($FJAM001, $FJAM002, $FJAM003 ...).

It is useful to make further entries for $FJAM0*nn* in addition $FJAM001. In this way, it is possible to execute several requests simultaneously. In the case of SNA links, you should always ensure that a sufficient number of entries are made.

The number of parallel executable file transfer requests issued in the local system is dependent on two factors:

- the number of local TS applications $FJAM0*nn* and
- the value of the operating parameter *maxosp*, which the FT administrator specifies with the *fta* command.

The lowest value determines the actual number of locally issued asynchronous requests that can be executed in parallel.

Example

With the specification *fta -o=4* (*maxosp=4*), you can simultaneously process up to four asynchronous requests with initiative in the local system. This means that you must enter four TS applications $FJAM0*nn* ($FJAM001, $FJAM002, $FJAM003 and $FJAM004), as well as $FJAM.

The entries with the symbolic names (GLOBAL NAMES) must be made for the transport systems used (as TSEL specification of the transport system). An entry must be made for each transport system via which requests are to be routed; no entry need be made for transport systems which are not used. The entry must be made in TRANSDATA format (indicator *T*). Depending on the version of CMX, the way in which the T selector is to be specified may differ for individual types of link. See the examples in the relevant CMX manual for further details.

- With station links, the name of a CMX station from the PDN generation must be specified, via which the communication with this application is to be handled. This CMX station must not already be assigned to another define application.
- With the TCP/IP-LAN transport system and when using CMX in the local system, two entries must be made for the symbolic name:
  - an RFC1006 entry with the transport selector. Enter the relevant symbolic name ($FJAM, $FJAM0nn where $01 \leq nn \leq 99$) as transport selector. The entry must be made TRANSDATA format (indicator *T*).
  - a LANINET entry with the port number. The port number is specified in ASCII format. The following convention must be observed:

    $FJAM Port number 1100
    $FJAM0nn Port number 11mm where: $01 \leq nn \leq 99$ and $01 \leq mm \leq 99$

  The port numbers for $FJAM001, $FJAM002 etc., unlike the symbolic names, need not be assigned in ascending order without gaps. They need only lie within the prescribed value range and must not be assigned more than once.
- With SNA links via TRANSIT, the name of the logical unit (LU name) and the associated LOCADDR (LU-No) must be specified for the CMX applications in each case. These values must correspond to the VTAM/NCP generation of the SNA system (LU statement) for this processor and with the configuration of TRANSIT in this processor (LOCADDR of the LUs assigned for *open*FT).

If you are working with *tnsxcom*, you must make the entries in a defined format (see samples).

Sample entries for *open*FT

```
$FJAM\
 TSEL    STANEA  T'FJMSINIX'   ; entry for STA1/MSV1
 TSEL    WANNEA  T'$FJAM'      ; entry for WAN-NEA,WAN-NX25,
                               ; ISDN-NEA,ISDN-NX25
 TSEL    WANSBKA T'$FJAM'      ; entry for WAN-CONS, ISDN-CONS
 TSEL    LANSBKA T'$FJAM'      ; entry for ETHN-CLNS/passive
                               ; necessary with link to CMX V3.0
 TSEL    OSITYPE T'$FJAM'      ; entry for ETHN-CLNS/active
 TSEL    LANINET A'1100'       ; entry for TCP/IP
 TSEL    RFC1006 T'$FJAM'      ; entry for TCP/IP-RFC1006
 TSEL    EMSNA   T'FJMFTSIN' 46; entry for TRANSIT-LU0
 TSEL    TRSNA   T'$FJAM'      ; entry for TRANSIT-LU6.2
$FJAM001\
 TSEL  STANEA  T'A01SINIX'     ; entry for STA1/MSV1
 TSEL  WANNEA  T'$FJAM001'     ; entry for WAN-NEA,WAN-NX25,
                               ; ISDN-NEA,ISDN-NX25
 TSEL  WANSBKA T'$FJAM001'     ; entry for WAN-CONS, ISDN-CONS
 TSEL  LANSBKA T'$FJAM001'     ; entry for ETHN-CLNS/passive
                               ; necessary with link to CMX V3.0
 TSEL  OSITYPE T'$FJAM001'     ; entry for ETHN-CLNS/active
 TSEL  LANINET A'1101‘         ; entry for TCP/IP
 TSEL  RFC1006 T'$FJAM001'     ; entry for TCP/IP-RFC1006
 TSEL  EMSNA   T'A01FTSIN' 47  ; entry for TRANSIT-LU0
 TSEL  TRSNA   T'$FJAM001'     ; entry for TRANSIT-LU6.2
$FJAM002\
           ...
```

3.2.3 Definition of the local TS application for *open*FT-FTAM

If you wish to use *open*FT-FTAM, the local application $FTAM must be defined. This is done automatically during initial installation or full installation, and also for update installation if no $FTAM entry is present. This application is used for all request with FTAM partners (outbound and inbound).

Special points

With the TCP/IP-LAN transport system, two entries must be made for the symbolic name:

- an RFC1006 entry with the transport selector. Enter the relevant symbolic name $FTAM as transport selector. The entry must be made TRANSDATA format (indicator *T*).
- a LANINET entry with the port number. The port number is specified in ASCII format.

More details on this topic can be found in the CMX manual and in “Appendix” on page 165.

You must make the entry in a defined format (see samples).

The GLOBALE NAME $FTAM is fixed. `T'$FTAM'` is recommended for the transport selector. The entries `PSEL V''` and `SSEL V''` are absolutely necessary.

Sample entries for *open*FT-FTAM

```
$FTAM\
 PSEL    V''                    ; empty presentation
 SSEL    V''                    ; empty session selector
 TSEL    WANSBKA T'$FTAM'       ; entry for WAN-CONS, ISDN-CONS
 TSEL    LANSBKA T'$FTAM'       ; entry for ETHN-CLNS/passive
                                ; necessary for link to CMX V3.0
 TSEL    OSITYPE T'$FTAM'       ; entry for ETHN-CLNS/active
 TSEL    RFC1006 T'$FTAM'       ; entry for TCP/IP-RFC1006
 TSEL    LANINET A‘4800‘        ; entry for TCP/IP
```

3.2.4 Definition of a remote TS application for *open*FT

All partner systems which are accessible via TCP/IP can be reached via the TCP/IP host name or the Internet address, possibly supplemented with a port number. In this case, it is sufficient to make a standard entry with the GLOBAL NAME *ftstd* for all partners which you wish to address.

In the case of ISDN links by means of the ISO transport protocol, it is also possible to enter ISDN number directly at the user interface. In this case, it is sufficient to make a standard entry with the GLOBAL NAME *ftstdisdn* for all partners which you wish to address in this manner.

In *open*FT partners with version 8.1 and later, you must ensure that the name, by which requests are processed with this partner, correspond to the instance ID of the remote system. If there is any doubt, a TNS input, whose global name is the instance ID, is needed.

For each further partner system which is to be accessible for requests issued locally, it is necessary to make a TNS entry. In both of the cases described above, additional TNS entries must be made for the partner systems, and separate names assigned to the partner systems. The entries are made in the menu system or translated using the TNS compiler *tnsxcom*.

As symbolic name (GLOBAL NAME), you must use an alphanumeric name containing up to 78 characters. No special characters may be used, except for::

- "." as separator
- "#" . The entry behind the hash "#" is used to differentiate entries with the same prefix. In this way, it is possible to enter a partner (who has several addresses) several times with the same name (prefix). This is only useful for inbound requests. Here, the partner system is always displayed with the same partner address (corresponding to the prefix).

You are free to select the symbolic name. However, it must be unique in the local system. The further entries to be made depends on the how the remote system is connected to the network. The entries must be made in TRANSDATA format (indicator *T*). You can obtain the information required to make the entries from the network administrator.

Standard entry for TCP/IP

If a Domain Name Service (DNS) is enabled on the network (default for all Web users), then using domain names would be advantageous, since no reconfiguration on the side of *open*FT is required when IP addresses are reconfigured on the partner systems. In order to be independent of the host names as well, it may be useful to assign aliases for applications (e.g. sales.company.com) in the DNS.

If TCP/IP host names from the */etc/hosts* file or DNS/NIS are to be used as partner names, or if the partner is to be address via the Internet address, a TNS entry with the name *ftstd* must be present. This entry must contain the Internet address 255.255.255.254.

Since only one *ftstd* entry may be present, the RFC1006 variant, as well as the port number and the transport selector most often used should be chosen for this standard entry.

Sample

```
ftstd\
       TA  RFC1006 255.255.255.254   PORT 1100 T‘$FJAM‘
```

Only the port number may be changed in this entry. It is strongly recommended that the port number 1100 be retained.

ftstd is a marker for all processors entered in the */etc/hosts* file or the DNS/NIS. With this entry, it is possible to use a the host names and alias names defined instead of the symbolic processor names. In this way, it is possible to identify a system not only on the basis of the individual TNS entry, but also via the *ftstd* entry in conjunction with the entries in the */etc/hosts* file or in the DNS/NIS (provided that the protocol variant (e.g. RFC1006) of the local *ftstd* entry corresponds to the entry in the remote system).

Inbound, the first name in the */etc/hosts* file is always displayed for the remote system. If it is longer than 8 characters, the display is truncated to 7 characters, followed by an asterisk (*). For example, the name *wallenstein* is displayed as *wallens**.

ftstd modifications do not be come effective until *open*FT has been terminated and restarted.

Standard entry for ISDN

If a partner system is accessible via ISDN, it can also be addressed directly by specifying ISDN numbers. In this case, a TNS entry with the name *ftstdisdn* must be present.

Sample

```
ftstdisdn\
         TA WANSBKA E.164  0  T'$FJAM'  2/2  WAN 1
```

You may make the standard entry *ftstdisdn* either only for *open*FT partners, or only for FTAM partners. In the example above, you can therefore only use the ISDN numbers to address *open*FT partners.

Special points

- With SNA links via TRANSIT, the VTAM application name (FJM*ftid*) corresponding to the VTAM generation of the SNA system (APPL statement) must be specified for the remote SNA partner system (*open*FT for OS/390 and z/OS). The processor number and region number are irrelevant for *open*FT, null (0) must be entered here in each case.
- With the TCP/IP-LAN transport system in the local system, you must enter the Internet address, the transport selector, as well as the port number of the partner processor. RFC1006 partner systems which support port 102 (e.g. BS2000/OSD and UNIX with CMX V5.0) are assigned the port number 102; all other partner systems are given the port number specified in the particular partner system for the $FJAM application.

3.2.4.1 Sample entries for *open*FT partners

- Entry of a PCMX partner dress for transfer via TCP/IP-RFC1006 and a PCMX, CMX-V4.0 or Windows partner (as of FT-PCD V2.6):

```
ftrfc\
        TA      RFC1006 123.4.5.67     PORT 1100 T'$FJAM'
;                       Internet addr. Portno    T selector
```

- Entry of variable Internet addresses for one and the same partner with the name *mobile* (e.g. a Notebook used from different locations and thus connected via
different Internet addresses):

```
mobile\
        TA      RFC1006 100.22.33.45     PORT 1100 T'$FJAM'
;                       Internet-addr1.  Portno   T selector
mobile#1\
        TA      RFC1006 101.20.30.40     PORT 1100 T'$FJAM'
;                       Internet addr2.  Portno   T selector
mobile#2\
        TA      RFC1006 102.21.31.41     PORT 1100 T'$FJAM'
;                       Internet-addr3.  Portno   T selector
```

- Entry of a partner address (*open*FT for BS2000/OSD partners) for transfer via TCP/IP-RFC1006 (Port 102):

```
ftbs2\
        TA      RFC1006 123.4.5.68     T'$FJAM'
;                       Internet addr. T selector
```

- Entry of a partner address for transfer via ETHN-CLNS/active:

```
ftethna\
        TA      OSITYPE 49+006C080015304050FE T'$FJAM'
 ;                      OSI network addr. T selector
```

(OSI network address as per ISO Standard 8348/Add.2, the structure is described in the CMX manual.)

- Entry of a partner address for transfer via ETHN-CLNS/passive:

```
ftethnp\
        TA      LANSBKA 080014110960  T'$FJAM'
 ;                      Ethernet addr. T selector
```

- Entry of a partner address for transfer via STA1/MSV1

```
ftmsv\
        TA      STANEA T'$FJAM'    18/18           WAN 1
;                     T selector  Proc./region    WAN CC
```

- Entry of a partner address for transfer via WAN-NEA, WAN-NX25, ISDN-NEA, ISDN-NX25

```
ftwannea\
        TA      WANNEA T'$FJAM'    1/18            WAN 2
;                      T selector  Proc./region    WAN CC
```

- Entry of a partner address for transfer via WAN-CONS, ISDN-CONS

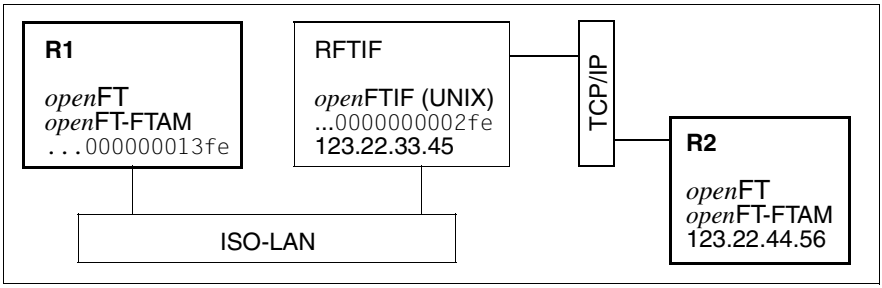
```
ftcons\
        TA     WANSBKA X.121 45890012233 T'$FJAM'  WAN 3
;                        SNPA info       T Sel.    WAN CC
```

- Entry of a partner address for transfer via TRANSIT-LU0

```
ftsna\
        TA     EMSNA T'FJMSNAXY' 0/0
;                    T selector  Proc./region
```

3.2.4.2 *open*FTIF example for UNIX-UNIX link via *open*FT protocol

In the following example, the two UNIX processors R1 and R2 are linked with the aid of a gateway computer RFTIF (with *open*FTIF (UNIX) software) via an ISO-LAN and a TCP/IP-N network. File transfer is possible in both directions between the two processors. CMX V5.0 is used on all processors.



The section below describes all TNS entries in the processors R1, R2 and RFTIF required for file transfer between R1 and R2.

TNS entries in processor R1:

```
$FJAM\
     TSEL    OSITYPE T'$FJAM'
$FJAM_OUTBOUND\
      TSEL    OSITYPE T'$FJAMOUT'
ftr2\
      SSEL   A'FTIFR2' TA OSITYPE
      470058+0144450100000123134500000000002fe T'FJMFTIF0'
```

TNS entries in processor RFTIF:

```
FJMFTIF0\
      TSEL  OSITYPE T'FJMFTIF0'
      TSEL  RFC1006 T'FJMFTIF0'
A01FTIF0\
      TSEL  OSITYPE T'A01FTIF0'
      TSEL  RFC1006 T'A01FTIF0'
ftifr2\
      TA    RFC1006 123.22.44.56  T'$FJAM'
ftifr1\
  TA   OSITYPE 470058+0144450100000123134500000000013fe T'$FJAM'
```

TNS entries in processor R2:

```
$FJAM\
      TSEL    RFC1006 T'$FJAM'
$FJAM_OUTBOUND\
      TSEL    RFC1006 T'$FJAMOUT'
ftr1\
      SSEL    A'FTIFR1'
      TA      RFC1006 123.22.33.45  T'FJMFTIF0'
```

3.2.5 Definition of remote TS applications for *open*FT-FTAM

For each FTAM system which is to be accessible for requests issued locally, or for which the automatic restart is to be provided, a TNS entry must be made. For FTAM partners, you must specify the presentation and session selectors. This only works for CMX V5.0 when you are using *tnsxcom* or the CMX GUI. The presentation/session and transport selector entries can be made in ASCII (A'...'), EBCDIC (E'...'), TRANSDATA format (T'...') or hexadecimal (X'...'). Presentation and session selectors may only be between 0 and 16 bytes long. If the presentation or session selector is missing, the entries `PSEL V''` or `SSEL V''` are absolutely necessary. With transport addresses for FTAM partners, no CC list may be specified.

Standard entry for ISDN

If a partner system is accessible via ISDN, it can also be addressed directly by specifying ISDN numbers. In this case, a TNS entry with the name *ftstdisdn* must be present

Example

```
ftstdisdn\
         PSEL   V''
         SSEL   V''
         TA     WANSBKA E.164  0  T'$FTAM'  2/2  WAN 1
```

You may make the standard entry *ftstdisdn* either only for *open*FT partners, or only for FTAM partners. In the example above, you can therefore only use the ISDN numbers to address FTAM partners.

Special points

- With the TCP/IP-LAN transport system in the local system, you must enter the Internet address, the transport selector, as well as the port number of the partner processor. RFC1006 partner systems which support port 102 (e.g. BS2000/OSD and UNIX with CMX V5.0) are assigned the port number 102; all other partner systems are given the port number specified in the particular partner system for the $FTAM application.
- The entries of the file to be translated with *tnsxcom* must in principle look the same as in the following example.

Checklist

The following checklist is intended to help you gather the data required for the TNSX entry of an FTAM partner. The questions must be answered by the FTAM partner.

1. openFT-FTAM sets up the connection.

   Which values do the following parameter have (with specification of coding):

a)	called X121/ LAN address/ NSAP/X.31	_____		
b)	called TSEL	_____	Code:	_____
c)	called SSEL	_____	Code:	_____
d)	called PSEL	_____	Code:	_____
e)	Protocol Identifier (Layer 3 CUD)	_____		
f)	called APT	_no _____NILAPTitle __ [1)]		
g)	called AEQ	_no _____ [1)]		
h)	calling APT	_no _____NILAPTitle __ [1)]		

[1)] APT (Application Process Title) and AEQ (Application Entity Qualifier) are not specified in the TNS entries, but in the *open*FT commands. Some FTAM partners expect APTs and possibly AEQs; others expect no APTs/AEQs to be specified.

2. The partner sets up the connection.

   Which values do the following parameters have (with specification of coding):

a)	calling X121/ LAN address/ NSAP/X.31	_____		
b)	calling TSEL	_____	Code:	_____
c)	calling SSEL	_____	Code:	_____
d)	calling PSEL	_____	Code:	_____

You must observe correct notation (uppercase and lowercase) and remember that blanks and X‘00‘ must be specified correctly for selectors.

Entries for a link to processor *BLUE* via X.25

- The partner requires the selectors in ASCII format. It does not require a protocol identifier.

```
blue\
   PSEL    A'FTAMBLUE'
   SSEL    A'FTAMBLUE'
   TA      WANSBKA 45890000001 A'FTAMBLUE'
```

- The following entry is necessary when processor *BLUE* has the initiative. It is used only to identify the initiator (sender check).

```
blue#1\
   PSEL    A' '
   SSEL    A'P'
   TA      WANSBKA 45890000001 A'@'
```

Entries for a link to processor *DEX* via X.25

- The partner requires the selectors in ASCII format, it does not require a protocol identifier. The partner just sends empty selectors when it has the initiative.

```
dex\
   PSEL    A'TS'
   SSEL    A'TS-SSAP'
   TA      WANSBKA 45890000001 A'TS-TSAPEAF' X'03010100'
```

- The following entry is necessary when processor *DEX* has the initiative. It is used only to identify the initiator.

```
dex#1\
   PSEL    V''
   SSEL    V''
   TA      WANSBKA 45890000001 V''   X'03010100'
```

3.2.5.1 Sample entries for FTAM partners

- Entry of a partner address for transfer via TCP/IP-RFC1006. The partner supports the standardized port number 102 of RFC1006.

```
ftamrfc\
     PSEL    V''
     SSEL    V''
     TA      RFC1006  123.4.5.67      T'$FTAM'
;                     Internet addr.  T selector
```

- Entry of a partner address (*open*FT for Windows with FTAM functionality) for transfer via TCP/IP-RFC1006 (Port 4800) :

```
ftamwnt\
    PSEL    V''
    SSEL    V''
    TA      RFC1006  123.4.5.68     PORT 4800    A'SNI-FTAM'
;                    Internet addr  Portno       T selector
```

- Entry of a partner address for transfer via ETHN-CLNS/active:

```
ftametha\
    PSEL    V''
    SSEL    V''
    TA      OSITYPE 49+006C080015304050FE T'$FTAM'
 ;                       OSI network addr. T selector
```

(OSI network address as per ISO Standard 8348/Add.2; the structure is described in the CMX manual.)

- Entry of a partner address for transfer via ETHN-CLNS/passive:

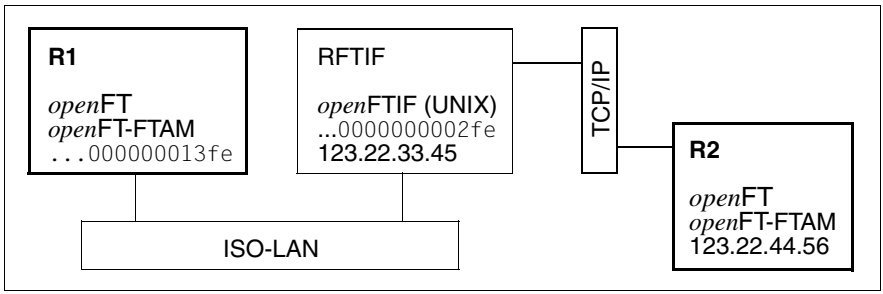
```
ftamethp\
    PSEL    V''
    SSEL    V''
    TA      LANSBKA 080014110960  T'$FTAM'
 ;                 Ethernet addr.T selector
```

- Entry of a partner address for transfer via WAN-CONS, ISDN-CONS

```
ftamcons\
    PSEL    V''
    SSEL    V''
    TA      WANSBKA X.121 45890040034 T'$FTAM' X'D5000002'
 ;                        SNPA info    T sel.   TPI
```

3.2.5.2 *open*FTIF sample for UNIX-UNIX link via FTAM protocol

In the following example, the two UNIX processors R1 and R2 are linked with the aid of an RFTIF gateway processor (with *open*FTIF (UNIX) software) via an ISO-LAN and a TCP/IP network. File transfer is possible in both directions. CMX V5.0 is installed in both processors.



All TNS entries in the processors R1, R2 and RFTIF required for file transfer between R1 and R2 are described.

TNS entries in processor R1:

```
$FTAM\
 PSEL   V''
 SSEL   V''
 TSEL   OSITYPE T'$FTAM'
ftamr2\
 SSEL  A'ftifr2'
 TA OSITYPE 470058+0144450100000123134500000000002fe T'FJMFTIF0‘
```

TNS entries in processor RFTIF:

```
FJMFTIF0\
 TSEL   OSITYPE T'FJMFTIF0'
 TSEL   RFC1006 T'FJMFTIF0‘'
ftifr2\
 SSEL   V''
 TA     RFC1006 123.22.44.56  T'$FTAM'
ftifr1\
 SSEL   V''
 TA    OSITYPE 470058+0144450100000123134500000000013fe T'$FTAM'
```

TNS entries in processor R2:

```
$FTAM\
 PSEL    V''
 SSEL    V''
 TSEL    RFC1006 T'$FTAM'
ftamr1\
 PSEL    V''
 SSEL    A'ftifr1'
 TA      RFC1006 123.22.33.45  T'FJMFTIF0'
```

3.3 Linking *open*FT for UNIX to *open*FT for OS/390 and z/OS via an SNA network

A UNIX system can interoperate with *open*FT for OS/390 and z/OS either via the TRANSDATA network and TRANSIT-SNA/CD or via a direct connection to the SNA network via TRANSIT. The required generation is describe below for both cases. It is also possible to set up a link to *open*FT for OS/390 and z/OS via a TCP/IP network.

3.3.1 Sample generation for the link TRANSIT

The FT identification of *open*FT for UNIX (ftid) is “FTSX”, that of the *open*FT for OS/390 and z/OS “MVS1”.

The processor name of the *open*FT for UNIX specified in the *fta -p=...* command is PDN001. The station name of the *open*FT for UNIX specified in the *fta -l=...* command is PCSTAT.

Please note, that the $FJAM_OUTBOUND entry must be removed and be replaced by the entries $FJAM001, $FJAM002,....

CMX generation:

```
$VERSION 5.0
$FJAM\
      TSEL      EMSNA T'FJMFTSX' 12
$FJAM001\
      TSEL      EMSNA T'A01FTSX' 13
$FJAM002\
      TSEL      EMSNA T'A02FTSX' 14
FJMMVS1\
      TA        EMSNA T'FJMMVS1' 0/0
```

NCP generation:

```
*
*
TRANSGRP GROUP ...
*
L48      LINE  ADDRESS=(48,FULL),...
*
PU48     PU    PUTYPE=2,                          -
               ADDR=C1,                           -
               MAXDATA=265,                       -
               MAXOUT=7,                          -
               PACING=3
*
*        LU FOR OPENFT (UNIX)
*
FJMFTSX  LU    LOCADDR12,                         -
               MODETAB=MODMSP,                    -
               DLOGMOD=FJMLMOD
*
A01FTSX  LU    LOCADDR=13,                        -
               MODETAB=MODMSP,                    -
               DLOGMOD=FJMLMOD
*
A02FTSX  LU    LOCADDR=14,                        -
               MODETAB=MODMSP,                    -
               DLOGMOD=FJMLMOD
```

This *open*FT for UNIX system is entered as follows in the network description book of the *open*FT for OS/390 and z/OS:

```
FJADDSYS REMSYS=FTSINIX2,SYSADR=(PDN001,PCSTAT),RELADR=FJMFTSX
```

In the UNIX system, the character string FJMMVS1 is specified as *processor name* in the remote *open*FT for OS/390 and z/OS in the ft and ncopy commands.

As required, the CHECK= parameter of the FJMODPAR command can be set to YES both in *open*FT for OS/390 and z/OS and in the UNIX system FTAC without restriction. The same *open*FT for UNIX system can (via a second data transmission controller and a second line) be connected to another FT system (e.g. *open*FT for BS2000/OSD, but not *open*FT for OS/390 and z/OS.

3.3.2 Sample generation for the link to *open*FT for OS/390 and z/OS via TRANSIT-CD without TRANSIT

The UNIX system is generated as a processor.

- The FT identification of *open*FT for UNIX (ftid) is “SXCD”, that of the *open*FT for OS/390 and z/OS “MVS1”.
- The processor name specified for the connection to the TRANSDATA network (processor link) in the *fta -p*=... command with *open*FT for UNIX is PCMX.
- The processor name of the preprocessor in which TRANSIT-CD is generated, is PDN002.
- The remote *open*FT for OS/390 and z/OS is located in the z/OS processor with processor number 3 and region number 28.

CMX generation:

The local application is entered in exactly the same way as for *open*FT for UNIX, which is (only) linked to *open*FT for BS2000/OSD via TRANSDATA.

In addition, the remote *open*FT for OS/390 and z/OS system must be entered as “remote TS application”:

```
FJMMVS1\
     TA     EMSNA T'FJMMVS1' 3/28
```

PDN generation:

```
            .
            .
            .
************************************************************
* DEFINITION * APPLICATION PCMX                             *
************************************************************
*
         XAPLG APLGNAM=PCMX
*
************************************************************
*        APPLICATION FOR openFT                             *
************************************************************
*
         XSTAT STATTYP=AP,                                   -
               STATNUM=460,                                  -
               STATNAM=$FJAM
*              IBMNAM=FJMSXCD,
*              IBMTYP=AP,
*              PACING=3
*
************************************************************
*        APPLICATION (nn=01) FOR openFT                     *
************************************************************
*
         XSTAT STATTYP=AP,                                   -
               STATNUM=461,                                  -
               STATNAM=$FJAM001
*              IBMNAM=A01SXCD,
*              IBMTYP=AP,
*              PACING=3
*
************************************************************
*        APPLICATION (nn=02) FOR openFT                     *
************************************************************
*
         XSTAT STATTYP=AP,                                   -
               STATNUM=462,                                  -
               STATNAM=$FJAM002
*              IBMNAM=A02SXCD,
*              IBMTYP=AP,
*              PACING=3
*
            .
            .
            .
```

For the z/OS processor:

The following entries are required in the PDN for the *open*FT for OS/390 and z/OS system:

```
           .
           .
*************************************************************
*     DEFINITION *APPLICATIONFJMMVS1                        *
*************************************************************
*
         XAPLG APLGNAM=FJMMVS1
*
*************************************************************
*        APPLICATION FOR openFT for OS/390 and z/OS         *
*************************************************************
*
         XSTAT STATTYP=AP,                                    -
               STATNUM=200,                                   -
               STATNAM=FJMMVS1
*              IBMNAM=FJMMVS1,
*              IBMTYP=FT3,
*              PACING=3
*
*************************************************************
*   APPLICATION (nn=01) FOR openFT for OS/390 and z/OS      *
*************************************************************
*
         XSTAT STATTYP=AP,                                    -
               STATNUM=201,                                   -
               STATNAM=A01MVS1
*              IBMNAM=A01MVS1,
*              IBMTYP=FT3,
*              PACING=3
*
*************************************************************
*   APPLICATION (nn=02) FOR openFT for OS/390 and z/OS      *
*************************************************************
*
         XSTAT STATTYP=AP,                                    -
               STATNUM=202,                                   -
               STATNAM=A02MVS1
*              IBMNAM=A02MVS1,
*              IBMTYP=FT3,
*              PACING=3
*
           .
           .
```

This *open*FT system is entered in the network description manual of the *open*FT for OS/390 and z/OS as follows:

```
FJADDSYS REMSYS=FTSINIX3,SYSADR=(PDN002,PCMX),RELADR=FJMSXCD
```

In the UNIX system, the character string FJMMVS1 is specified in the ft and ncopy commands as *processor name* for the remote *open*FT for OS/390 and z/OS.

In this case, the CHECK= parameter of the FJMODPAR command can be set to YES as required in the *open*FT for OS/390 and z/OS. All required sender checks can also be carried out in the UNIX system.

4 Administering *open*FT via SNMP

In order to administrate *open*FT via SNMP, your processor must be have a EMANATE master agent.

The *open*FT subagent is available for the Reliant Unix, Solaris/Sparc, HP-UX and UnixWare platforms. It is supplied with *open*FT and is set up when *open*FT is installed.

4.1 Activities after installation

After installation of *open*FT, different activities are required.

1. If your system is not already being administered with SNMP, you will need to activate administration via SNMP.

   You will need a community string with write authorization to administer *open*FT via the *open*FT subagent. If you only have read authorization, then only information can be output via SNMP. In this case you will not be able to change values (or perform starts or stops, see also page 73).

   Consult your UNIX documentation to find out how to activate the SNMP administration.

2. Start the agent (see below)

You will find a list of activities performed by the SNMP administrator in the documentation for the management station used.

Consult your SNMP documentation to obtain information on security mechanisms.

4.2 Starting the *open*FT subagent

There are two ways to start the *open*FT subagent:

- Enter `/opt/bin/ftagt &`.

  The *open*FT subagent is then started and remains active until the system is shutdown.

- Remove the comment symbol in the line of the startup file that contains the word *ftagt* (for example: */var/openFT/std/etcinit/openFTinst* under Reliant UNIX) as well as in the corresponding line in the startup file of any other instances. The *open*FT subagent is then also started each time the system is booted.
  If you want to terminate the *open*FT subagents for some reason, then you can do this with a *kill -2* command with the process number of the *open*FT subagent as the parameter.

Note that SNMP can only work with one instance when clustered. The decisive factor is which instance is set up to start when the agent is started (see also section “Using openFT in a cluster” on page 22).

4.3 SNMP management for *open*FT

The *open*FT subagent is used to:

- obtain information about the status of *open*FT
- start and stop *open*FT
- obtain information about system parameters
- modify system parameters
- create the new public key for encryption
- output statistical data
- to control the diagnosis

The MIB to *open*FT offers objects for the above-mentioned management tasks. It is located in the file */opt/openFT/snmp/openFT.asn1*.

The objects for starting and stopping, encrypting the public key, modifying the system parameters and controlling the diagnose require write access.

4.3.1 Starting and stopping *open*FT

MIB definition

Object name	Access	TransView interface
ftStartandStop ftStartandStopFTAM	read-write read-only	*open*FT protocol FTAM protocol

Entry

Syntax	Integer	Meaning
on off	3 4	*open*FT/FTAM is started *open*FT/FTAM is stopped

Setting the values “on” or “off” causes the *open*FT subagent to start or stop *open*FT. Write access supplies information about the current status of the FT system.

4.3.2 System parameters

MIB definition

Object name	Access	TransView interface
ftSysparVersion	read-only	Version
ftSysparTransportUnitSize	read-write	Transport Unit Size
ftSysparMaxOSP	read-write	Max OSP
ftSysparMaxISP	read-write	Max ISP
ftSysparProcessorName	read-write	Processor Name
ftSysparStationName	read-write	Station Name
ftSysparCode	read-write	Code Table
ftSysparMaxInboundReqs	read-write	Max Inbound Requests
ftSysparMaxLifeTime	read-write	Max Life Time

The explanation of the possible values in the description of the *fta* command starting on page 85.

4.3.3 Statistical information

MIB definition

Object name	Access	TransView interface
ftStatLocked	read-only	Requests in status LOCKED
ftStatWait	read-only	Requests in status WAIT
ftStatActive	read-only	Requests in status ACTIVE
ftStatCancelled	read-only	Requests in status CANCELLED
ftStatFinished	read-only	Requests in status FINISHED
ftStatHold	read-only	Requests in status HOLD
ftStatLocalReqs	read-only	Local requests
ftStatRemoteReqs	read-only	Remote requests

The individual states have the following meanings:

LOCKED
The request is temporarily excluded from processing.
This state may occur both for *open*FT and for FTAM partners.
With *open*FT partners, e.g. when a resource bottleneck is encountered or when external data media must be made available.
With FTAM partners, when one of the partners proposes a waiting period until the next start or recovery attempt via the FTAM protocol, and this period exceeds the delay normally permitted.

WAIT
The request is waiting.

ACTIVE
The request is currently being processed.

CANCELLED
The request was cancelled in the local system. However, the remote system is aware of its existence, e.g. because it was previously active. Therefore, the request cannot be removed from the request queue until a connection to the partner has been re-established.

FINISHED

This status arises for requests involving FTAM partners when the request has been either completed or cancelled, but the user has not yet been informed of the fact

HOLD

The start time specified when the request was issued has not been reached

4.3.4 Control of diagnostics

MIB definition

Object name	Access	TransView interface
ftDiagStatus	read-write	Diagnose Management

Entry

Syntax	Integer	Meaning
off on	1 18	Diagnosis management is deactivated Diagnosis management is activated

4.3.5 Public key for encryption

MIB definition

Object name	Access	TransView interface
ftEncryptKey	write-only	

Entry

Syntax	Integer	Meaning
create-new-key	1	A new public key is created.

5 *open*FT commands for the administrator

This chapter contains the commands which are available only to the administrator or which include more options for the administrator than the user.

5.1 Overview of the commands

Command	Function	Note
fta	Set operating parameters Start and exit *open*FT Toggle trace mode on and off Set the logging scope Create a new key	FT administrator only
ftalarm	Report failed requests	FT administrator only
ftc	Delete asynchronous requests	FT user also [1) 2)]
ftcrei	Create an instance	FT administrator only
ftcrep	Create FT profile	FT user also [1) 3)]
ftdeli	Delete an instance	FT administrator only
ftdell	Delete log record	FT or FTAC administrator only
ftdelp	Delete FT profile	FT user also [1)]
ftexpe	Export FT profiles and admission sets into file	FTAC administrator only
fti	Display information	FT user also [1) 2)]
ftimpe	Import FT profiles and admission sets from a file into the local system	FTAC administrator only
ftlang	Set language interface (must be called with `/opt/openFT/bin/ftbin/ftlang`)	FT administrator only
ftmoda	Modify admission set	FT user also [1)]
ftmodi	Modify an instance	FT administrator only
ftmodp	Modify FT profile	FT user also [1) 3)]
ftmodr	Change the order of the requests in the request queue	FT user also [1)]
ftrs	Delete requests unconditionally	FT administrator only
ftshwa	Display admission sets	FT user also [1)]
ftshwd	Display diagnostic records	FT or FTAC administrator only

Command	Function	Note
ftshwe	Display FT profiles and admission sets from file	FTAC administrator only
ftshwl	Display log records	FT user also [1)]
ftshwp	Display FT profiles	FT user also [1)]
ftupdi	Update the instance directory	FT administrator only
ftupdk	Update the public keys	FT administrator only
install.ftam	Install *open*FT-FTAM	FT administrator only

1) This command is also available to users with restricted functional scope.

2) This command is described only in the User Guide.

3) This command is described in detail in the User Guide for *open*FT V8.1. This manual describes only the switches and values that offer you additional options as an administrator.

As the **administrator**, you may execute the commands listed below with the additional options to perform the corresponding action **system-wide**. This means that:

You can use *ftc* to delete any desired file transfer requests.

You can use *ftcrep* to create FT profiles for any login names

You can use *ftdelp* to delete any FT profiles.

You can use *fti* to obtain information on all requests in the request queue, independent of the login name.

You can use *ftmoda* to modify any of the admission sets.

You can use *ftmodp* to modify any of the FT profiles.

You can use *ftmodr* to change the order of all requests in the request queue independent of the login name.

You can use *ftshwa* to display any of the admission sets.

You can use *ftshwl* to display any of the log records.

You can use *ftshwp* to display any of the FT profiles.

5.2 Notational conventions

The command syntax essntially corresponds to the output that you get when you specify the command with *-h* option. The following conventions have been used for syntax diagrams:

< > angle brackets are used for parameters which you may replace with current values. You must not specify the angle brackets < > and the permissible value ranges.

[ ] enclose optional entries. The effect on the function of the command is described for the individual parameters.

␣ stands for at least one blank that must be inserted between the various entries. You may also enter more than one blank.

| stands for alternatives. You may specify only one of the values indicated.

Lengths and characters sets

The values which you use for parameters in the commands must observe certain restrictions on length and on the characters available:

file name

the file name can be specified as either absolute or relative, file names in the local and remote system must not be longer than 512 characters. On the other hand, long file names (>128) are not possible at the program interface. If the file name contains blanks, they must be set in quotation marks (e.g. "file name"). If the remote system requires quotation marks around the file name, these must not be canceled (e.g. ‘file name’) as on the shell level.

date

numeric; exactly 8 characters in the form `yyyymmdd` with:
`yyyy` for year, `mm` for month and `dd` for day

Note that for all date entries in *open*FT V8.1 commands, you may only specify values up to and including 20380120 (January 20, 2038)

user id

login name, up to 32 characters
(first 8 characters unique)

command
: up to 500 characters; for follow-up processing commands, the commands for success or failure must not be longer than 500 characters in total

partner
: partner name, alphanumeric (a..z, A..Z, 0..9) and the special characters "%", "." and ",", up to 78 characters. For partners using *open*FT V8.1 or later, the partner's instance ID should be used. For this to work, the instance ID must be either a valid DNS name of a partner system which is accessible via TCP/IP, or the partner's address must be entered in the TNS, where the global name of the TNS entry is the partner's instance ID. You can also specify the partner name in various ways:
  – as a TNS name (all 5 parts of the name are supported)
  – as a TCP/IP host name (if the *ftstd* entry exists)
    a port number can be specified after the host name. It is separated from the host name by a colon (:*port*).
  – as an IP address (if the *ftstd* entry exists); with or without the prefix %ip:
    – with the prefix %ip (e.g. %ip139.22.33.44)
      In this case, the partner name is treated directly as an IP address. This approach enhances performance.
    – without prefix (e.g. 139.22.33.44)
      In this case, the TNS is searched first, followed by the file */etc/hosts*. If no matching entry is found there, the path name is treated as an IP address.

    A port number can be specified after the IP address just like for the TCP/IP host name. It is separated from the IP address by a colon (:*port*).
  – as an ISDN address with the prefix % or %ISDN (if the *ftstdisdn* entry exists)

profile name
: alphanumeric (a..z, A..Z, 0..9), up to 8 characters

transfer admission
: The transfer admission may contain only printable characters and must not start with a hyphen; minimum of 8 characters, maximum of 67 characters (in UNIX systems, up to 16 characters).

Special characters in the entries for *file name, file name-prefix*, *transfer admission*, *user ID*, *account*, *password*, *follow-up processing* (see notes on the commands) must be escaped using a backslash (\). Here, you must differentiate between special characters for file transfer and UNIX special characters, and escape the special characters accordingly.

Example

The account number 1111111,00000000,88888888 is specified in the transfer admission. The comma is a special character that enables file transfer to distinguish the elements of the triple, and must therefore be escaped with a backslash (\). This reverse slash is also a special character for the shell, and must therefore also be escaped. The entry then appears as follows:

“1111111\\,00000000\\,88888888”

The **sequence** of entries in the command is arbitrary, except for the entries for
– the source and destination of a request (e.g. local and remote file name, partner name,...)
– the authorization to access the remote system, i.e., the transfer admission or the system login.

When there is a large number of parameters, *open*FT commands can be very long. If you want to use the keyboard to enter commands that are longer than 256 characters, you will need to work with continuation lines. You can obtain these by entering the sequence \ ↵.

Note that the entries for follow-up processing must be enclosed in single or double quotes (' or ").

If the entry for follow-up processing also contains single quotes (’), it is recommended to enclose the entire entry in double quotes ("). The single quotes in the follow-up processing command (e.g. single quotes in a BS2000 password) can then be written as expected in the partner system (such as BS2000).

Some FT commands have a very extensive syntax. To avoid having to look up the syntax in this manual all the time, you can also have the syntax of any given command displayed on the screen using the *-h* option.

5.3 Output in CSV format

For some Show commands, *open*FT for UNIX offers output in CSV format. CSV (**C**omma **S**eparated **V**alues) is a popular format in the PC environment in which tabular data is defined by lines. Output in CSV format is offered for the following commands:

– fti
– ftshw
– ftshwa
– ftshwe
– ftshwl
– ftshwp

Many programs such as spreadsheets, databases, etc., can import data in CSV format. This means that you can use the processing and presentation features of such programs on the data output by the above commands.

The output fields are described under the respective commands.

Every record is output as a line, and each record contains information on an object. The first line is always the header and contains the field names of the respective columns. **Only the field names are guaranteed, not the order of fields in a record**. In other words, the order of columns is determined by the order of the field names in the header line. Fields within an output line are separated by semicolons (;).

The following data types are differentiated in the output:

Number

String
: Since the ";" character has a special meaning in the CSV output as a field separator, any text containing a ; (semicolon) is enclosed within double quotes.
Keywords are never enclosed within double quotes and **always** begin with the character *.

Date
: Date and time are always output in the format `yyyy-mm-dd hh:mm:ss`; a date alone is output in the format `yyyy-mm-dd`.

One example of a possible evaluation procedure is supplied as a reference template in the Microsoft Excel format in the file */opt/openFT/samples/ftaccnt.xlt*. The template evaluates a CSV log file by means of an automatically running macro. The result shows the number of inbound and outbound requests and the Kilobytes transferred in each case for all users.

5.4 fta - Administer *open*FT

Using *fta*, you can set operating parameters for *open*FT, start and exit *open*FT, create new keys for encrypted data transfer and switch on and off trace mode for error diagnosis. You will find a detailed description of encryption in section “AES encryption method” on page 20.

You can define the maximum number of asynchronous requests *open*FT is to execute simultaneously. You can also define the maximum length of the blocks to be transferred, and the range of file transfer requests to be logged by *open*FT.

In order to process asynchronous requests issued by a local or remote system, *open*FT must be started using the *fta* command. Otherwise, *open*FT will only execute synchronous requests and will store asynchronous requests issued by the local system in the request queue.

All *open*FT parameters are stored in a disk file. They are thus available in their original form the next time the system is started up.

Format

```
fta  -h  |
        [ -s | -t]
        [ -k] [ -dk=<key reference 1..9999999>]
        [ -n | -f]
        [ -kl=0 | 768 | 1024] [ -sd=n | y]
        [ -u=<block length 512..65535>]
        [ -o=<maxosp 0..200>] [ -i=<maxisp 0..200>]
        [ -p=<processor name 1..8>] [ -l=<station name 1..8>]
        [ -id=<identification 1..64>]
        [ -iq=<Number of inbound requests per partner 0..2000>]
        [ -ql=<Request lifetime 1..400>]
        [ -co=1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 13 | 14 | 15 | 16]
        [ -lt=a | f | n] [ -lc=a | m | r]
        [ -d=m | c] [ -tb=n | f]
        [ -ae=y | n]
```

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

-s *open*FT is started. After starting *open*FT, an *fta -s* process is run. If FTAM is also used, two *fta* processes are present after start. You can specify whether you wish to use FTAM during installation.

When starting *open*FT the protective bit setting is set for all files which are created by inbound requests. The protective bit setting is taken from the shell under which the *fta -s* command is entered.

-t *open*FT is exited.

Unconditional termination of all activities. All active connections are first cleared down.
Requests present in the request queue are processed normally after *open*FT has restarted. Requests which were aborted on termination of *open*FT are executed after restart, provided that the partner supports this function.

When the *fta -t* command has been issued, *open*FT can only be started again if all server processes are terminated. This may take some time, for example, if the connection cleardown is delayed by line problems.

-k This option can be used to create a new key pair set at any time. This option is supported as of *open*FT V8.0 for compatibility reasons only. Because of the length of the key, a new key pair set is no longer created on a regular basis like this.

-dk=<key reference 1..99999999>
Using this switch, you can delete the key pair set with the specified reference. After this, your system can no longer be authenticated by partner systems which are still using the accompanying public key. If you delete the last key pair set in your system, your openFT can no longer encrypt either request data or file content.

-n The monitoring function is activated. When activated, the diagnostic data are written to the trace files located in the directory */var/openFT/instance/traces* and (when linked to *open*FT partners) can be evaluated with the *fttrace* service program. Here *instance* means the name of the corresponding instance.A description of the evaluation of trace files is given starting on page 156.

-f The monitoring function is deactivated.

-kl=0 | 768 | 1024

The *-kl* parameter can be used to change the length of the RSA key used in encryption. The value of the *kl* parameter specifies the new RSA key length in bits. The RSA key is only used for the encryption of the AES key agreed between the partners (or for encrypting the DES key in versions up to *open*FT V7.0).
*open*FT uses the AES key for encrypting request description data and any file content present.
Encryption can be explicitly disabled using kl=0. The *fta -kl=...* command can be specified in current *open*FT operation.

When the request queue is created, *kl=768* is used as the default value.

-sd=n | y

With this option you can enable a special *open*FT response to allow inbound SNA requests via a dialup connection *(*sd = **S**NA **d**ialup connection).

n SNA dialup connection is disabled (default setting). If *maxisp=1* is set (*fta -i=*), then SNA inbound requests are also permitted via a dialup connection.

y SNA dialup connection is enabled. If *maxisp > 1* is set (*fta -i=*), then you must specify *fta -sd=y* because otherwise a request will not get to the transfer phase. Setting *maxisp > 1* may be necessary due to connections to other types of partners.

The call can be issued at any time and takes effect immediately. Even when the option is enabled, connections can be established to SNA partners (even if they are not connected via a dialup connection), but only one connection can be established for each SNA partner. The result of the *fta -sd=...* call is stored at remains stored even after a restart.
The *SNA dialup connection* setting (yes or no, corresponding to *fta -sd=y | n)* is not shown in the *fti -p* output.

-u=block length

Defines the maximum length of the blocks to be transferred within the range 512 up to maximum value of 65535. This upper limit is required, since the NEABF protocol elements SAC and SDK are not fragmentable and the maximum possible length of these protocol elements has increased as a result of the increased *open*FT key lengths (up to 1024 bits).

The default is 65535 characters.

The block length is only valid for requests involving *open*FT partners.

-o=maxosp
: Maximum number of requests issued locally (outbound), that can be processed simultaneously. The default value is 4.
Restriction for FTAM partners: the maximum limit for the number of connections that can be active at the same time is half the number of files that a process can open simultaneously.
The sum of *maxosp* and *maxisp* may not exceed 200 (128 for station and SNA links).

-i=maxisp
: Maximum number of requests issued remotely (inbound), that can be processed simultaneously. The maximal value depends on the CCP used (see CCP manuals). The default value is 12.
he sum of *maxosp* and *maxisp* may not exceed 200 (128 for station and SNA links).

-p=processor name
: You specify the processor name assigned to your system here. If your system is linked to *open*FT for OS/390 and z/OS via TRANSIT-SINIX, your specification must comply with the value for SYSADR in the *open*FT for OS/390 and z/OS network description file for your system.

-l=station name
: The station name of the *open*FT application. The default value is $FJAM.

The specifications for *processor name* and *station name* depend on how your system is connected to the network. Further details can be found in the chapter chapter “Installation and configuration” on page 31.

-id=identification
: Specifying the instance identification of your *open*FT instance. Partner systems using *open*FT Version 8.1 and later, address your system via this string. In return, *open*FT uses the instance ID as the sender address when addressing the partners. The instance ID must be unique and not case-sensitive (see also section “Instance Identifications” on page 25).
If you modify the instance ID, the relevant public key files will be automatically updated.

-iq= Number of inbound requests per partner
: This setting is only valid for requests involving FTAM partners. Here you specify the maximum number of inbound entries in the request queue per partner; the default value is 64, but any value between 0 and 2000 is permitted. By limiting the number of entries per partner, you prevent a partner from filling the request queue with its own requests and thus blocking other partners.

-ql=Request lifetime)

Here you specify the maximum lifetime of entries in the request queue (in days); the default value is 30, but any value between 1 and 400 days is permitted. Both outbound and inbound requests in the request queue are deleted after the specified time span. In the case of outbound requests, this value can be combined with the *-ct*=... option in the *ft* command.

-co=1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 13 | 14 | 15 | 16

This option is used to set a new character set, which is represented by a code table. The default code table is ISO 8859-1; this setting can be modified if required by specifying a numerical value for -co in the corresponding variant of the ISO 8859 character set.

The code table specification is only valid for *open*FT requests. If the partner system does not support the code table you used, the request will be canceled and a corresponding error message will be issued.

-lt=a | f | n

This option is used to selectively deactivate FT log records.
With connections to FTAM partners, it can take up to a minute for the selection to become active.

a (all)

This is the default setting; log records are written for all FT requests.

f (failure case)

Log records are written for failed FT requests only.

n (none)

No log records are written.

-lc= a | m | r

This option is used to selectively deactivate FTAC log records.
With connections to FTAM partners, it can take up to a minute for the selection to become active.

a (all)

This is the default setting; log records are written for all FTAC access checks.

m (modifying FM calls)

Log records are written for all FTAC access checks on modifying file management requests issued by the remote system, and on rejected FTAC access checks

r (reject case)
Log records are written for rejected FTAC access checks only

-d= m | c
With this option, you can determine the value used for output of the "Modification Date". *fta -d=* can be entered at any time and is effective immediately. This option only works for *open*FT partners.

m The value used for the "Modification Date" is the time at which the file transfer was created.

c The value used for the "Modification Date" is the time at which the file is stored after transfer (corresponds to the behavior of older FT versions).

-tb= f | n
This option allows you to activate/deactivate tabulator expansion and the conversion of blank lines into lines with one character for non-FTAM partners.
The following parameters are provided:

f (off)
Tabulator expansion and blank line conversion are deactivated.

n (on)
Tabulator expansion and blank line conversion are activated.

-ae=y | n
This option activates/deactivates the AET (Application Entity Title).

y A "nil Application Entity Title" is included as the calling or called Application Entity Title (AET) for transfer using the FTAM protocol (the default value corresponds to the behavior of FT Version 5.2)

n The AET is deactivated. The option only has to be reset to *-ae=n* if FTAM link partners, as responders, do not expect to receive an AET.

Examples

1. *open*FT is already installed and is now being started.

```
fta␣-s
fta: openFT V8.1 [including FTAM server] started.
```

2. *open*FT is to be started and the operating parameters set. *open*FT is installed on a system which has the DNS name *hugo.fusinet.at*. It should be possible to simultaneously process up to two requests issued locally.

```
fta␣-s␣-o=2␣-id=hugo.fusinet.at

fta: openFT V8.1 [including FTAM server] started.
```

3. The maximum length of the blocks to be transferred is 1024 bytes. started.

```
fta␣-u=1024

fta: openFT parameter(s) set.
```

4. Log records are written for failed FT requests only.

```
fta␣-lt=f

fta: openFT parameter(s) set.
```

5. Each FTAM partner is allowed 100 entries in the request log. All entries in the request log are deleted after eight days.

```
fta␣-iq=100␣-ql=8

fta: openFT parameter(s) set.
```

5.5 ftalarm - Report failed requests

The *ftalarm* command is used to trigger an alarm if, within two minutes, more FT requests than the number specified by the user fail. The failed FT requests are identified using the log file by means of a return code not equal to 0 for the FTAC log records. *ftalarm* uses the *cron* function.

A separate *ftalarm* call is required for each instance.
Proceed as follows: activate the instance with *ftseti*, and call *ftalarm*.

Format

ftalarm [-h |
-s <number of errors 1..99999999> |
-t]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

-s <number of errors>
starts the *ftalarm* function. When the specified *number of errors* in FTAC log records is exceeded within two minutes, the following message is output on the console and to the file */var/openFT/instance/log/conslog (*where *instance* means the name of the corresponding instance):

```
openFTalarm: number or more access control error loggings
within 2 minutes
```

The partial string *openFTalarm:* within this message is also guaranteed for future versions of *open*FT and can be interpreted for automatic processing by system management tools.

The messages are output by the *cron* function at regular intervals and can therefore be delayed by up to one minute when the *ftalarm* function is activated.

-t terminates the *ftalarm* function.

5.6 ftcrei - Create or activate an instance

The *ftcrei* command allows you to create a new instance or re-activate a deactivated instance.

When an instance is created, the instance file tree is linked to the */var/openFT* directory with the resources of an instance.

If the specified instance file tree does not yet exist, it is created.

When the instance file tree is created, the operating parameters, the profile files and the startup and shutdown files are initialized in the same way as for a new installation.

If the instance file tree already exists, *ftcrei* checks the version. If the instance file tree was created using an older version of *open*FT, it must first be updated using the *ftupdi* command before it can be reactivated.

Use of several *open*FT instances is only possible using the TCP/IP transport system. If you would like to use several instances, you must delete all openFT-specific TNS entries that are not TCP/IP compliant (i.e. all except for LANINET and RFC1006). You must explicitly assign an individual address to all instances using *-addr=*.

If the instance is to be authenticated in partner systems, it must have a unique instance ID assigned to it (using *fta -id=*). In addition, a public key for the instance must be made available to the partner systems.

Format

ftcrei -h |
<instance 1..8>
[<directory>]
[-addr=<host name>]

Description

-h Displays the command syntax. Anything specified after *-h* is ignored.

instance
Name of the instance to be created.
Instance names have a maximum length of 8 characters and must consist of alphanumeric characters. The first character must not be a number. The instance name must not be confused with the instance ID (see *fta -id=*).

directory

Directory in which the instance file tree is to be located.
By default, it is created in:

`/var/openFT/.instance`

-addr=host name

Internet host name by which the instance is addressed. If your system has a DNS name, you should specify the full DNS name. *open*FT then uses the first 8 characters of the first part of the name (the host name qualifier) as the processor name (*fta -p=*) and the entire name as the instance ID (*fta -id=*).

Messages of the ftcrei command

If *ftcrei* could not be executed properly, a self-explaining message is output. The exit code is not equal zero in this case.

Examples:

1. The instance *inst1* is to be newly created in the directory */cluster/inst1*. The DNS name is *hugo.abc.net*. The directory */cluster/inst1* is not allowed to exist.

   ```
   ftcrei inst1 /cluster1/inst1 –addr=hugo.abc.net
   ```

   Where the operational parameter *fta -p=* is *hugo* and *fta -id=* is *hugo.abc.net*.

2. The existing instance *inst2* from the directory */cluster/inst2* is to be re-activated. No host name may be specified.

   ```
   ftcrei inst2 /cluster/inst2
   ```

5.7 ftcrep - Create an FT profile

ftcrep stands for "create profile". This command can be used by any user to set up FT profiles for his or her login name.

The FTAC administrator can also set up FT profiles for other login names, either with or without defining a transfer admission.

Format

ftcrep -h |
<profile name 1..8>
<transfer admission 8..16> | @n
[-ua=[<user id 1..32> [ ], [<password 1..20> | @n]]]
[-v=y | -v=n] [-d=yyyymmdd]
[-u=pr | -u=pu]
[-priv=y | -priv=n]
[-iml=y | -iml=n]
[-iis=y | -iis=n] [-iir=y | -iir=n]
[-iip=y | -iip=n] [-iif=y | -iif=n]
[-ff=t | -ff=m | -ff=r | -ff=p | -ff=tmpr | -ff=prmt]
[-dir=f | -dir=t | -dir=ft]
[-pn=<partner name 1..78>,...,<partner name(50) 1..78> | -pn=]
[-fn=<file name 1..512> | -fn=]
[-fnp=<file name prefix 1..511>]
[-ls= | -ls=@n | -ls=<command1 1..500>]
[-lsp=<command2 1..499>] [-lss=<command3 1..499>]
[-lf= | -lf=@n | -lf=<command4 1..500> |]
[-lfp=<command5 1..499>] [-lfs=<command6 1..499>]
[-wm=o | -wm=n | -wm=e | -wm=one]
[-c=y | -c=n]
[-txt=<text 1..100>]

Description

In the following, only those switches and values are described, which are very important for the administrator or which offer the administrator additional options.

profile name
: is the name you wish to assign to the FT profile. This name can be used to address the FT profile, for example when it is to be modified or deleted. Be sure not to confuse the profile name with the transfer admission (see

below). The profile name must be unique among all the FT profiles under your login name, or FTAC will reject the *ftcrep* command and issue the message FT profile already exists. To have the profile names you have already assigned displayed, you can issue the *ftshwp* command (without options).

transfer admission | @n
: replaces the login authorization for your UNIX system otherwise required in FT requests. When this transfer admission is specified in an FT request, FTAC applies the access rights defined in this FT profile.

  transfer admission
  : The transfer admission must be unique within your UNIX system so that there are no conflicts with transfer admissions defined by other FTAC users with other access rights. If the transfer admission you select has already been assigned, FTAC rejects the *ftcrep* command and issues the message:
    `Transfer admission already exists.`

    As the FTAC administrator, you can assign a transfer admission for yourself under your own login name or for any other user. In this case, however, you must specify the entire login authorization (i.e. the login name and password for that login name) if you do not have root privileges (UID=0).

  @n for *transfer admission*
  : As the FTAC administrator, by specifying @n, you can create FT profiles for other login names without having to define transfer admissions. The owner of the login name for which the FT profile was created can then enable this profile using the *ftmodp* command. In order to do this, the owner must specify a transfer admission with *ftmodp*.

transfer admission not specified
: FTAC will then prompt you to enter the transfer admission. Your entry is not displayed to prevent unauthorized persons from seeing the transfer admission. To exclude the possibility of typing errors, the program expects you to enter the transfer admission a second time as an entry check.

-ua=[user id**,**[password | @n]]

FTAC administrators use *-ua* to specify the user IDs for which they want to set up FT profiles.

user id
: The user can specify only his own user ID.
As the FTAC administrator, you can specify any user ID.

,password
: specifies the password of the login name. The FT profile for the login name is only valid while the password is valid for the login name. If the password is changed, the profile can no longer be used.

If you want to assign an FT profile for another user and also assign a transfer admission for that profile, you must specify the login name as well as the password for that login name if you do not have root privileges (UID=0).

@n for *password*
: This entry may only be specified by the FTAC administrator. With *@n*, you cannot assign any transfer admission for the FT profile if you do not have root privileges (UID=0).

comma only (,) no *password* specified
: causes FTAC to query the password on the screen after the command is entered. Your entry is not displayed to prevent unauthorized persons from seeing the transfer admission. To exclude the possibility of typing errors, the transfer admission must be entered a second time.

user id only (without comma and no *password*) specified
: the profile is valid for all the passwords for *user id*.

-ua=␣ specified or *-ua* not specified
: the FT profile is created for the individual login name.

-priv=n | -priv=y
: is used by the FTAC administrator to grant privileged status to FT profiles. Possible values are:

n (default value)
: The FT profile is not privileged (initially).

y
: The FT profile is privileged.

-iml=y | -iml=n
-iis=y | -iis=n
-iir=y | -iir=n
-iip=y | -iip=n
-iif=y | -iif=n

These options are used to specify whether the FT profile is to be restricted by the values in the admission set (MAX. USER LEVELS). If the FT profile is also privileged by you as the FTAC administrator, the entries you have made (the MAX. ADM LEVELS) can also be ignored. This FT profile would then allow *inbound* basic functions which are disabled in the admission set to be used. Possible values are:

y allows the values in the admission set to be ignored.

n (default value)
restricts the functionality of the profile to the values in the admission set.

The following table shows which subcomponents of the file management can be used under which conditions.

Inbound file management function	**Values of the admission set or extension in profile**
Display file attributes	Inbound Send (IBS) enabled
Modify file attributes	Inbound Receive(IBR) **and** Inbound File Management(IBF) enabled
Rename files	Inbound Receive(IBR) **and** Inbound File Management(IBF) enabled
Delete files	Inbound Receive(IBR) enabled **and** Write mode = overwrite in profile
Display directories	Inbound File Management(IBF) enabled
Create, rename and delete directories	Inbound File Management(IBF) enabled **and** direction= from partner in profile

5.8 ftdeli - Delete or deactivate an instance

The *ftdeli* command allows you to delete an instance. Deleting an instance removes only the symbolic link in the local */var/openFT* directory. The instance file tree is not changed. The standard instance *std* and the currently set instance can not be deleted.

Format

ftdeli -h |
<instance 1..8>

Description

-h Displays the command syntax. Anything specified after *-h* is ignored.

instance
Name of the instance to be deleted.
Instance names have a maximum length of 8 characters and must consist of alphanumeric characters. The first character must not be a number.

Messages of the ftdeli command

If *ftdeli* could not be executed properly, a self-explaining message is output. The exit code is not equal zero in this case.

Examples

1. The instance *inst1* from the directory */CLUSTER/inst1* is to be deactivated on computer *CLUSTER1*, since it has been switched over to *CLUSTER2*. The directory */CLUSTER/inst1* is retained.

```
ftdeli inst1
```

2. Instance *inst2* with the directory */CLUSTER/inst2* is to be deleted along with the instance file tree.

```
ftdeli inst2
rm -r /CLUSTER/inst2
```

3. Using *ftseti*, it was changed to instance *inst3*. There, an attempt is being made to deactivate the instance *inst3*.

```
ftdeli inst3
ftdeli: openFT Instance 'inst3' can not be removed.
```

5.9 ftdell - Delete log record

With *ftdell*, you can delete FT log records for all login names This function is not permitted for the ordinary user.

Store the log records by redirecting the output of *ftshwl* to a file or to the printer (see section "ftshwl - Display log records" in the user manual).

Deleting log records changes the size of the file since the storage space is freed immediately after deletion.

The time by which the log records are to be deleted can be entered either as a fixed time with date and time or as a relative time; for example: all records before 10 days ago.

By default, *open*FT deletes all log records which are older than 30 days every time the system is started up.

Format

ftdell [-h] |
[-rg=[[[yyyy]mm]dd]hhmm | #1..99999999 | 0..999]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

-rg=[[[yyyy]mm]dd]hhmm
You use *-rg* to specify the end of a logging interval.
[[[yyyy]mm]dd]hhmm: When selecting the time, a 4-digit specification is interpreted as the time expressed in hours and minutes, a 6-digit specification as the day (date) and time in hours and minutes, an 8-digit specification as the month, day, and time in hours and minutes, and a 12-digit specification as the year, month, day, and time in hours and minutes. The largest possible value that can be specified as the date is 20380120 (January 20, 2038).
*open*FT then deletes all log records which are older that the specified time.
The optional data ([…]) is automatically replaced by current values.

-rg=0..999
Here you use *-rg* to specify a time interval (relative to the current date and time) as a multiple of 24 hours, i.e. number of days. The specification can be 1-3 digits long. *open*FT then deletes all log records which are older

than the specified time. This means you are looking back in time. If you specify *rg=2*, for example, all log records which are older than two days (48 hours) are deleted.

-rg=#1..99999999
: Here you use *-rg* to specify the end log ID. It is identified by a leading # character, followed by the 1-8-digit ID. *open*FT then deletes all log records which belong to this log ID or which have a smaller log ID.

-rg not specified
: The range is not a selection criterion, i.e. all log records are to be deleted by 00:00 hours of the current date.

Example

1. As the FT or FTAC administrator, you wish to delete all FT log records written up to 00:00 hours of the current date.

```
ftdell
ftdell: log records deleted.
```

2. As the FT or FTAC administrator, you wish to delete all FT log records written up to the current time:

```
ftdell -rg=0
ftdell: log records deleted.
```

3. As the FT or FTAC administrator, you wish to delete all log records written before the last 7-day period (7 times 24 hours before the current time:

```
ftdell -rg=7
ftdell: log records deleted.
```

4. As the FT or FTAC administrator, you wish to delete all log records from the beginning to the record with the log ID 1450:

```
ftdell -rg=#1450
ftdell: log records deleted.
```

5.10 ftdelp - Delete FT profiles

ftdelp stands for "delete profile". When checking your set of profiles (with *ftshwp*), it is a good idea to weed out, from time to time, those which are no longer needed and are merely taking up storage space.

ftdelp allows the FTAC administrator to delete FT profiles belonging to other login names as well. Of course, the administrator should first inform the owner of the profiles before deleting them.

Format

ftdelp -h |
<profile name 1..8> | @a
[-s=[<transfer admission 8..16>| @a |@n]
[,<user id 1..32> | @a]]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

profile name | @a
is the name of the FT profile you wish to delete.

@a for *profile name*
profile name is not used as a criterion for selecting the FT profile to be deleted. If you do not identify the profile more closely with *-s* (see below) you will delete all of your FT profiles.

-s=[transfer admission | @a | @n][,user id | @a]
-s is used to specify criteria for selecting the FT profiles to be deleted.

transfer admission
is the transfer admission of the FT profile to be deleted.

@a for *transfer admission*
deletes either the FT profile specified by *profile name* (see above) or all of your FT profiles.

As the FTAC administrator, you must specify *@a* if you want to delete FT profiles belonging to other login names, since you actually should not know the transfer admission.

@n for *transfer admission*
: As the FTAC administrator, you can specify *@n* if you only want to delete FT profiles of other login names, which do not have any defined transfer admissions.

transfer admission not specified
: causes to query the transfer admission on the screen after the command is entered. Your entry is not displayed to prevent unauthorized persons from seeing the transfer admission. To exclude the possibility of typing errors, the program prompts you to enter the transfer admission a second time. If you just press ↵, this has the same effect as specifying *@a*.

,user id
: As the FTAC administrator, you can specify any login name.

@a for user id
: If you specify *@a* as the FTAC administrator, FT profiles belonging to all login names are deleted.

user id not specified
: deletes only profiles belonging to the user's own login name, regardless of who issues the command.

-s not specified
: if *@a* is specified for *profile name*, all the FT profiles belonging to the login name under which the *ftdelp* command is issued are deleted. Otherwise, the FT profile with the specified name is deleted.

5.11 ftexpe - Export FT profiles and admission sets

ftexpe stands for "export environment", i.e. exporting the FTAC environment, or exporting FT profiles and admission sets.

Using *ftexpe* the FTAC administrator can write FT profiles and admission sets of any login names to files, thereby saving them.

However, the standard admission set is not saved and the variable values in an admission set (values marked with an asterisk (*)) that refer to the standard admission set, are saved as variables. This means that there is no fixed value for the relevant basic function in the backup. If an admission set is imported, the relevant basic function receives the value of the standard admission set that is currently valid.

FT profiles and admission sets saved in this way can be re-imported using the *ftimpe* command.

Format

ftexpe -h |
<file name 1..512>
[-u=<user id 1..32>,...,<user id(100) 1..32>]
[-pr=<profile name 1..8>,...,<profile name(100) 1..8> | -pr=@n]
[-as=y |-as= n]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

file name
With *file name*, you specify the name of the file in which the FT profiles and records are to be written. You may access this file only using the *ftimpe* and *ftshwe* commands. *path/file name* must not be longer than 512 characters, and no backup files with the same name must exist in the current directory.

-u=user id1[,user id2][,user id3]...
-u specifies the login names whose FT profiles and admission sets are to be saved to a file. Up to 100 login names can be specified simultaneously.

-u not specified
: all FT profiles and admission sets on the system are saved to the specified file.

-pr=profilname1[,profilname2][,profilname3]... | @n
: specifies the FT profiles to be saved to the specified file (up to 100).

@n for *profilname*
: no FT profiles are saved.

-pr not specified
: all FT profiles belonging to the login names specified in the -u parameter, are saved.

-as=y |-as= n
: specifies whether or not the admission sets should be saved to the specified file. Possible values are:

y (default value)
: all admission sets belonging to the login names specified in the *-u* parameter, are saved.

n
: no admission sets are saved.

Example

The admission set and the FT profiles belonging to the login name *donald* are to be saved. *ftacsave* is specified for the backup file.

```
ftexpe␣ftacsave␣-u=donald
```

5.12 ftimpe - Import profiles and admission sets

ftimpe stands for "import environment", i.e. importing the FTAC environment or importing FT profiles and admission sets. Using *ftimpe*, the FTAC administrator can import the FT profiles and admission sets of any login names from a file that was created using the *ftexpe* command.

Only those FT profiles whose profile names have not been specified for other FT profiles under the specified login name are imported.

An FT profile whose transfer admission has already been defined for another FT profile in the system will be imported, but has an undefined transfer admission. It must therefore be assigned a new transfer admission using the *ftmodp* command before it is used. If the existing FT profile in the system is designated as private, it is immediately disabled. It must be assigned a new transfer admission using the *ftmodp* command, before it is used.

The imported FT profiles are automatically locked and must be unlocked before use with the command *ftmodp* and the parameter *-v=y* if the FTAC administrator does not have root privileges (UID=0). Privileged FT profiles lose their privileged status when imported.

The standard admission set is not saved when it is exported. Therefore, the standard admission set on the computer at the time of importing remains valid. Variable values in the imported admission sets, that refer to the standard admission set (and are therefore marked with an asterisk (*), are assigned the value of the standard admission set that is currently valid.

Format

ftimpe -h |
<file name 1..512>
[-u=<user id 1..32>,...,<user id(100) 1..32>]
[-pr=<profile name 1..8>,...,<profile name(100) 1..8> | -pr=@n]
[-as=y |-as=n]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

file name
file name specifies the file from which the FT profiles and admission sets are to be imported.

-u=user id1[,user id2][,user id3]...
specifies the login names whose FT profiles and admission sets are to be imported. You can specify up to 100 login names simultaneously.

-u not specified
all FT profiles and admission sets are imported.

-pr=profile name1[,profile name2][,profile name3]...| -pr=@n
specifies the FT profiles to be imported (up to 100).

@n for *profile name*
no FT profiles are imported.

-pr not specified
all FT profiles belonging to the login names specified in the *-u* parameter are imported. However, the profile is not imported if another FT profile of the same name already exists under this login name.

-as=y | -as= n
specifies whether or not admission sets are to be imported. Possible values are:

y (default value)
all admission sets belonging to the login names specified in the *-u* parameter are imported.

n no admission sets are imported.

Example

The admission set and FT profiles of the login name *donald* were saved to the file *ftacsave* with *ftexpe*. They are to be imported to another system under the same login name.

```
ftimpe␣ftacsave␣-u=donald
```

You may receive the following messages, for example:

```
OWNER    NAME
donald   secret1     FT profile already exists.
         secret2
```

These messages indicate that *donald* has already created the FT profiles *secret1* and *secret2* on the new system, and these profiles were therefore not imported.

Note

If you wish to delete an admission set for a login name that does not exist, enter the command *ftmoda ␣login-name ␣-ml=s*. This situation can occur when you use *ftexpe* to incorporate into your system a file that has been created on a different host.

5.13 ftlang - Change default language setting

The default language for *open*FT is determined by evaluating the LANG environment variable during installation.

You can switch languages later on using the shell procedure */opt/openFT/bin/ftbin/ftlang*.
For more details see section “Switching the language interface” on page 11.

Format

ftlang [-h |
-i |
de |
en]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

-i you can use this switch to query the currently set language variant.

de *open*FT is switched to German as the default.

en *open*FT is switched to English as the default.

In both cases, the necessary messages files, the *fthelp* procedure, the manpages and the help texts of the graphical user interface are activated.

Example

The default language setting is switched from German to English:

```
/opt/openFT/bin/ftbin/ftlang␣en
```

5.14 ftmoda - Modify admission sets

ftmoda stands for "modify admission set". As the FTAC administrator, you can use this command to define settings for the standard admission set and for any admission set of any user in the system. The settings made by the administrator for other users are the MAX. ADM LEVELS.

You can release each basic function

– for all partner systems
– for only those partner systems that are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists)
– for only authenticated partner systems
– for no partner systems (i.e. block).

For basic functions, consult the table on page 115.

The FTAC administrator can also use *ftmoda* to make another login name the FTAC administrator.

In *open*FT V8.1, the meaning of the numbers in the admission set has been modified. Whereas in the old versions a **"1"** meant that the basic function could be used with all partners in the TNS, this is now represented by the value **"90"** in versions 8.1 and later.

*open*FT accepts and stores any whole number between 0 and 100 at the switches. The admissions check is carried out based on the next level down (0, 10, or 90). This means, for example, that a value of **"1"** blocks a basic function, since the check is based on **"0."**

Format

```
ftmoda -h |
        [ <user id 1..32> | @s ]
        [ -priv=y ]
        [ -ml=s | -ml=0..100 ]
        [ -os=s | -os=0..100 ]
        [ -or=s | -or=0..100 ]
        [ -is=s | -is=0..100 ]
        [ -ir=s | -ir=0..100 ]
        [ -ip=s | -ip=0..100 ]
        [ -if=s | -if=0..100 ]
```

Description

-h Displays the command syntax on the screen. Entries after the are ignored.

user id | @s
As the FTAC administrator, you can specify any login name desired.

@s for *user id*
By entering the value @s, the FTAC administrator can modify the standard admission set.

user id not specified
modifies the admission set of the login name under which *ftmoda* is entered.

-priv=y
As the FTAC administrator, you can assign administrator privileges to the specified *user id*.

-priv not specified
does not change the FTAC administrator.

-ml=s | -ml=0..100
sets the same value for all six basic functions.

Possible values are:

s sets each of the basic functions to the value defined in the standard admission set.

0 disables all of the basic functions.

10 All basic functions are only released for *open*FT partners that are authenticated in the local system.

90 All basic functions are released for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).

100 All basic functions are released for all partner systems. For outbound file management functions, no check is made.

-ml not specified
leaves the settings in the admission set unchanged if none of the following entries are made.

-os=s | -os=0..100
sets the value for the basic function *outbound send*, which determines whether or not requests initiated in your UNIX system can send data to a remote system.

s sets the value defined in the standard admission set.

0 disables the basic function *outbound send*.

10 The basic function *outbound send* is only released for *open*FT partners that are authenticated in the local system.

90 enables the basic function *outbound send* for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).

100 enables the basic function *outbound send* for all partner systems.

-os not specified
leaves the setting for *outbound send* unchanged.

-or=s | -or=0..100
sets the value for the basic function *outbound receive*, which determines whether or not requests initiated in your UNIX system can fetch data from a remote system.

s sets the value defined in the standard admission set.

10 The basic function *outbound receive* is only released for *open*FT partners that are authenticated in the local system.

90 disables the basic function *outbound receive*.

1 enables the basic function *outbound receive* for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).

100 enables the basic function *outbound receive* for all partner systems.

-or not specified
the value for *outbound receive* is not changed.

-is=s | -is=0..100
sets the value for the basic function *inbound send*, which determines whether or not a remote partner system can fetch data from your UNIX system.

s sets the value defined in the standard admission set.

0 disables the basic function *inbound send*.

The subcomponent of the basic function *inbound file management* for "displaying file attributes" is also disabled.

Any requests from remote FTAM partner systems to create a new file are also rejected.

10 The basic function *inbound send* is only released for *open*FT partners that are authenticated in the local system.

90 enables the basic function *inbound send* for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).

100 enables the basic function *inbound send* for all partner systems.

-is not specified
leaves the setting for *inbound send* unchanged.

-ir=s | -ir=0..100
sets the value for the basic function *inbound receive*, which determines whether or not a remote partner system can send data to your UNIX system.

s sets the value defined in the standard admission set.

0 disables the basic function *inbound receive*.

The subcomponents of the basic function *inbound file management*, deletion and renaming of files, as well as modification of file attributes, are also locked.

10 The basic function *inbound receive* is only released for *open*FT partners that are authenticated in the local system.

90 Enables the basic function *inbound receive* for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).

100 enables the basic function *inbound receive* for all partner systems.

-ir not specified
: leaves the setting for *inbound receive* unchanged.

-ip=s | -ip=0..100
: sets the value for the basic function *inbound follow-up processing + preprocessing + postprocessing*, which determines whether or not a remote system may request follow-up, pre- or postprocessing on your UNIX system.

  s sets the value defined in the standard admission set.

  0 disables the basic function *inbound follow-up processing + preprocessing + postprocessing*.

  10 The basic function *inbound follow-up processing + preprocessing + postprocessing* is only released for *open*FT partners that are authenticated in the local system.

  90 enables the basic function *inbound follow-up processing + preprocessing + postprocessing* for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).

  100 enables the basic function *inbound follow-up processing + preprocessing + postprocessing* for all partner systems.

-ip not specified
: leaves the setting for *inbound follow-up processing + preprocessing + postprocessing* unchanged.

-if=s | -if=0..100
: sets the value for the basic function *inbound file management*.

  s sets the value defined in the standard admission set.

  0 disables the basic function *inbound file management*.

  10 enables the basic function *inbound file management* only for *open*FT partners that are authenticated in the local system.

  90 enables the basic function *inbound file management* for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).

  100 enables the basic function *inbound file management* for all partner systems.

Please note that the subcomponent "display file attributes" is controlled via the basic function *send inbound*. Some subcomponents affect other settings (see the following table):

Inbound file management function	**Values of the admission set or extension in profile**
Display file attributes	Inbound Send (IBS) enabled
Modify file attributes	Inbound Receive(IBR) **and** Inbound File Management(IBF) enabled
Rename files	Inbound Receive(IBR) **and** Inbound File Management(IBF) enabled
Delete files	Inbound Receive(IBR) enabled **and** Write mode = overwrite in profile
Display directories	Inbound File Management(IBF) enabled
Create, rename and delete directories	Inbound File Management(IBF) enabled **and** direction= from partner in profile

-if not specified

leaves the setting for *inbound file management* unchanged.

5.15 ftmodi - Modify an instance

The *ftmodi* command allows you to assign another Internet host name address to an instance.

Format

ftmodi -h |
<instance 1..8>
[-addr=<host name> | @n]

Description

-h Displays the command syntax. Anything specified after *-h* is ignored.

instance
Name of the instance to be modified.
Instance names have a maximum length of 8 characters and must consist of alphanumeric characters. The first character must not be a number.

-addr= host name | **@n**
Internet host name by which the instance is addressed.

host name
Another Internet host name can be assigned to the instance here.

@n for *host name*
This specification is only permitted for the standard instance *std*.

The standard instance is not assigned a host address anymore, and therefore it signs on for all addresses of the system.

In this manner you can switch from an operation with several instances to a one instance operation.

Messages of the ftmodi command

If *ftmodi* could not be executed properly, a self-explaining message is output. The exit code is not equal zero in this case.

5.16 ftmodp - Modify FT profiles

ftmodp stands for "modify profile". The FTAC administrator can use this command to change or to privilege FT profiles of other users.

In the event that the FTAC administrator does not have any root admission, then admission profiles of other users are blocked after a modification (except after *-priv=y*). This can be by-passed by entering *-ua=user id,password*. If the user later changes his/her password, the profile will no longer be usable without further modification.

Format

```
ftmodp -h |
        <profile name 1..8> | @a
        [ -s=[<transfer admission 8..16> | @a | @n ][,<user id 1..32> | @a]]
        [ -ua=[ <user id 1..32> ],[<password 1..20> | @n ] ]
        [ -nn=<profile name 1..8> ]
        [ -tad= | -tad=<transfer admission 8..16> | -tad=@n ]
        [ -v=y | -v=n ]     [ -d=[yyyymmdd | -d=]
        [ -u=pr | -u=pu ]   [ -priv=y | -priv=n ]
        [ -iml=y | -iml=n ]
        [ -iis=y | -iis=n ]   [ -iir=y | -iir=n ]
        [ -iip=y | -iip=n ]   [ -iif=y | -iif=n ]
        [ -ff= | -ff=t | -ff=m | -ff=r | -ff=p | -ff=tmrp | -ff=prmt ]
        [ -dir=f | -dir=t | -dir=ft ]
        [ -pn=<partner name 1..78>,...,<partner name(50) 1..78> | -pn=]
        [ -pna=<partner name 1..78>,...,<partner name(50) 1..78> ]
        [ -pnr=<partner name 1..78>,...,<partner name(50) 1..78> ]
        [ -fn=<file name 1..512> | -fn=] [ -fnp=<file name prefix 1..511>]
        [ -ls= | -ls=@n | -ls=<command1 1..500> ]
        [ -lsp= | -lsp=[<command2 1..499>] [ -lss= | -lss=command3 1..499>]
        [ -lf= | -lf=@n | -lf=<command4 1..500> | ]
        [ -lfp= | -lfp=<command5 1..499>] [-lfs= | -lfs=<command6 1..499>]
        [ -wm=o | -wm=n | -wm=e | -wm=one ]
        [ -c=y | -c=n]
        [ -txt=<text 1..100> | -txt=]
```

Description

In the following, only those options and values which are particularly important for the administrator or which offer the administrator additional functionality are described in detail. The remaining options are described in the User Guide.

profile name
: specifies the name of the FT profile you wish to modify. To see the profile names you have already assigned, you can issue the *ftshwp* command (without options).

  @a for profile name
  : modifies all FT profiles that come into question at once, unless you select a specific profile with the option *-s*.

-s=[transfer admission | @n | @a] [,user id | @a]
: is used to specify selection criteria for the FT profile to be modified.

  transfer admission
  : specifies the transfer admission of the FT profile to be modified.

  @a for *transfer admission*
  : modifies either the FT profile specified with *profile name* (see above) or (if no profile name was specified) all the profiles that come into question.

  @n for *transfer admission*
  : selects all FT profiles without transfer admission.

  transfer admission not specified
  : causes to query the transfer admission on the screen after the command is entered. Your entry is not displayed to prevent unauthorized persons from seeing the transfer admission. To exclude the possibility of typing errors, the program prompts you to enter the transfer admission a second time. If you just press ↵, this has the same effect as specifying *@a*.

  ,user id
  : As the FTAC administrator, you can specify any login name here.

  @a for *user id*
  : If you specify *@a* as the FTAC administrator, you can modify the FT profiles for any login names.

  user id not specified
  : modifies only profiles belonging to the user's own login name, regardless of who issues the command.

-s not specified

if *@a* is specified for *profile name*, all the FT profiles belonging to the login name under which the *ftmodp* command is issued are modified. Otherwise, the FT profile with the specified name is modified.

-ua=[user id],[password | @n]

With *-ua*, the FTAC administrator can assign any desired FT profile of a login name to another login name.

user id

As the FTAC administrator, you can specify any login name here.

,password

specifies the password for a login name. The FT profile for the login name is valid only so long as the password *password* is valid for the login name. When the password is changed, the profile can no longer be used (not locked!).

@n for *password*

In this case, the FTAC administrator cannot specify any transfer admission for the FT profile if you do not have root privileges (UID=0). An existing transfer admission will be automatically deleted in this case.

comma only (,) no *password* specified

causes FTAC to query the password on the screen after the command is entered. Your entry is not displayed to prevent unauthorized persons from seeing the transfer admission. In this case, single quotes must not be escaped by a backslash. To exclude the possibility of typing errors, the program prompts you to enter the transfer admission a second time.

user id only (without comma and *password*) specified

means that the profile is valid again for all passwords of the specified login name *user id*.

-ua=␣not specified

the login name of this FT profile remains unchanged.

-tad=[transfer admission | @n]
allows you to modify the transfer admission of an FT profile. As the FTAC administrator, you can also modify the transfer admissions for other login names if you have root privileges (UID=0).

transfer admission
The transfer admission must be unique within your UNIX system so that there are no conflicts with transfer admissions defined by other FTAC users for other access permissions. If the transfer admission you select has already been assigned, FTAC rejects the *ftmodp* command and issues the message
`Transfer admission already exists.`

@n for *transfer admission*
disables the old transfer admission.

transfer admission not specified
-tad= causes FTAC to prompt you to enter the transfer admission after the command has been entered. Your entry is not displayed to prevent unauthorized persons from seeing the transfer admission. To exclude the possibility of typing errors, the program expects you to enter the transfer admission a second time as an entry check.

-tad not specified
does not modify the transfer admission of the FT profile.

-priv=y | -priv=n
This option is used by the FTAC administrator to grant privileged status to an FT profile.

y grants privileged status to the FT profile. The FT administrator's entries in the admission set are ignored for requests executed with a privileged FT profile, i.e., if the user uses the *-iml, -iis, -iir, -iip* or *-iif* options in the FT profile, both the user' s entries (MAX. USER LEVELS) and the administrator' s entries (MAX. ADM LEVELS) are ignored.

n withdraws the privileged status, if it had been granted, from the FT profile.

-priv not specified
does not modify the privileged status of the FT profile.

-iml=y | -iml=n
-iis=y | -iis=n
-iir=y | -iir=n
-iip=y | -iip=n
-iif=y | -iif=n

These options are used to specify whether the FT profile is to be restricted by the values in the admission set (MAX. USER LEVELS). If the FT profile is also privileged by you as the FTAC administrator, the entries you have made (the MAX. ADM LEVELS) can also be ignored. This FT profile would then allow *inbound* basic functions which are disabled in the admission set to be used. Possible values are:

y allows the values in the admission set to be ignored.

n (default value)
restricts the functionality of the profile to the values in the admission set.

-ixx not specified
The existing definitions of the profile for the basic functions involved remain in effect.

The following table shows which subcomponents of the file management can be used under which conditions.

Inbound file management function	**Values of the admission set or extension in profile**
Display file attributes	Inbound Send (IBS) enabled
Modify file attributes	Inbound Receive(IBR) **and** Inbound File Management(IBF) enabled
Rename files	Inbound Receive(IBR) **and** Inbound File Management(IBF) enabled
Delete files	Inbound Receive(IBR) enabled **and** Write mode = overwrite in profile
Display directories	Inbound File Management(IBF) enabled
Create, rename and delete directories	Inbound File Management(IBF) enabled **and** direction= from partner in profile

5.17 ftmodr - Change the order of requests in the request queue

With the *ftmodr* command, you can change the priority of requests you have issued, or of a group of requests, for example all the requests to a particular partner. Furthermore, you have the option of changing the order of requests within a priority.

As the FT administrator, you can change the priority of all requests in the system.

Format

ftmodr -h |
-id=<transfer id 1..32767> |
-s=<partner 1..78> | @a[,<user id 1..32> | @a]
[-pr=n | l] [-qp=f | l]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

-id=transfer id
Number of an individual file transfer request for which the priority and/or position is/are to be changed in the request queue (without leading nulls). This number is displayed on the screen when a request is accepted, but can also be displayed with the *fti* command. Note that you must also specify the operands *-pr* and/or *-qp* with this option and that the *-s* option cannot be specified concurrently.

-s=partner | @a [,user id | @a]
Selects specific requests for which the priority is to be changed, e.g. all requests to a particular partner. The operand *-pr* must also be specified. Note that this option cannot be used in combination with *-qp* and/or *-id*.

partner
The priority of all requests which you have issued to this partner system is changed. *partner* is a name for the partner system up to 78 characters in length. For partners using *open*FT V8.1 or later, the partner's instance ID should be used here. For this to work, the instance ID must be either a valid DNS name of a partner system which is accessible via TCP/IP, or the partner's address must be

entered in the TNS, where the global name of the TNS entry is the partner's instance ID. You can also specify the partner name in various ways:

- as a TNS name (all 5 parts of the name are supported)
- as a TCP/IP host name (if the *ftstd* entry exists);
  a port number can be specified after the host name. It must be separated from the host name by a colon (:*port*).
- as an IP address (if the *ftstd* entry exists); with or without the prefix %ip:
  - with the prefix %ip (e.g. %ip139.22.33.44)
    In this case, the partner name is treated directly as an IP address. This approach enhances performance.
  - without prefix (e.g. 139.22.33.44)
    In this case, the TNS is searched first, followed by the file */etc/hosts*. If no matching entry is found there, the partner name is treated as an IP address.

  A port number can be specified after the IP address just like it can be for the TCP/IP host name; it must be separated from the IP address by a colon (:*port*).
- as an ISDN address with the prefix %, %isdn or %ISDN (if the *ftstdisdn* entry exists)

A distinction is made between uppercase and lowercase.

With requests to FTAM partners, you may specify an Application Entity Title (AET) in the computer name. This is sent to the partner as a "called AETitle" and interpreted there.

@a for *partner*
: By specifying *@a* for the *partner*, all requests issued to remote systems are changed.

,user id | @a
: As the FT administrator, you can enter a user ID here to change the priority of FT requests that were sent under that user ID and directed to the system specified under *partner*.

@a for *user id*
: By specifying *@a*, you can change the priority of requests for all users in the system. Simultaneous specification of a request number is not permissible.

user id not specified
: The priority of own requests is changed, regardless who entered the command.

-pr=n | l
: indicates the new priority. The following values are possible:

  n (normal)
  : the request has the priority "normal"

  l (low)
  : the request has the priority "low"

-qp= f | l
: indicates the position of the request within the same priority. The following values are possible:

  f (first)
  : the request is placed at the top of the list of requests with the same priority

  l (last)
  : the request is placed at the bottom of the list of requests with the same priority.

Note

For FTAM partners, the order of request processing does not correspond to the order for output of the *fti* command. Changing the position or priority does not immediately affect the order of request processing.

5.18 ftrs - Delete requests unconditionally

While requests are currently being processed, a situation may arise in which it is possible to establish a normal connection between the local and the remote FT system. In this case, you can use the command *ftrs* to delete asynchronous requests system-specifically.
This command may only be used in cases of emergency, since inconsistencies may otherwise occur in the request queue of the remote partner system. It is reserved for the FT administrator.

The *ftrs* command is used to delete all requests for a specific remote system from the request queue. This may be practical for example, if your partner system has been dismantled, but requests still remain in the request queue.

Caution

- Unconditional deletion should be used with extreme caution, particularly for requests with FTAM partners. Outbound requests can always be deleted using the *ftc* command, provided a connection exists to the partner or can be re-established at a later stage. You should only use *ftrs* if this option is no longer available or if only inactive inbound requests exist for this partner.
- If requests for FTAM partners are removed from the local request queue using this type of delete request but are not removed from the remote request queue due to a connection fault, then the requests remain in the remote request queue until their maximum lifetime is reached or until they are deleted by the FT administrator of the remote system, if indeed either of these options is available on the remote partner.

Before you issue the delete request for an *open*FT partner, you must ensure that *open*FT is not started and the requests to be deleted are not in the request queue of the FT partner system.

FTAM requests can be deleted even if *open*FT has been started, except during the start and end phase of *open*FT.

To delete all requests, *open*FT must be exited beforehand.

When the request has been deleted, a result message is output.

Format

ftrs -h |
-p=<partner 1..78>

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

-p=partner
The *partner* is specified as it is given in the request queue. The *fti -q* command places the processor name in the F-SYSTEM column of the output. If the character * is specified for *processor name*, all requests are deleted from the request queue. Remember that the asterisk (*) must be escaped, e.g. using a backslash (*).
If an application entity title was specified for request to an FTAM partner, this application entity title must also be specified for the *ftrs* command. Information can be obtained using the long form of the *fti* command. Refer to the user manual for an explanation of the application entity title.

Example

All requests to the remote system *bs2r1* are to be deleted.

```
ftrs␣-p=bs2r1
ftrs: Number of deleted requests: 10.
```

5.19 ftshwa - Display admission sets

ftshwa stands for "show admission set", and allows you to examine admission sets.

As the FTAC administrator, you can obtain information on all admission sets in your system.

It outputs the following information:

- which basic functions the owner of the login name has enabled or disabled,
- which basic functions the FTAC administrator has enabled and disabled for this login name,
- whether or not the admission set is privileged (i.e. who is the FTAC administrator).

Format

ftshwa -h |
[<user id 1..32> | @a | @s] [-csv]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

user id | @a | @s
specifies the user id of for which the admission set is to be displayed.

user id
As the FTAC administrator, you can specify any login name desired.

If a login name longer than 8 characters is specified, the first 7 characters are output followed by an asterisk (*).

@a for *user id*
When entered by the FTAC administrator, *@a* displays information on the standard admission set and all admission sets that differ from it.

@s for *user id*
returns information only on the standard admission set.

If you specify a non-existent login name for *user id*, the current standard admission set is displayed.

user id not specified
FTAC displays information on the admission set of the login name under which *ftshwa* was entered.

-csv Specifying *-csv* indicates that the FT admission sets are to be output in the CSV format. The values in the output are separated by semicolons.

-csv not specified
The FT admission sets are output in the standard format.

Example

Display of command `ftshwa␣@a`:

```
$ ftshwa @a

               MAX. USER LEVELS              MAX. ADM LEVELS          ATTR
USER-ID  OBS  OBR  IBS  IBR  IBP  IBF  OBS  OBR  IBS  IBR  IBP  IBF
*STD     100  100  100  100  100  100  100  100  100  100  100  100
john     100* 100* 100* 100* 100* 100* 100* 100* 100* 100* 100* 100*
 root      90   90   10   10   10   10  100* 100* 100* 100* 100* 100* PRIV
 smith     90   90    0    0    0   90  100* 100* 100* 100* 100* 100*
```

The displayed information has the following meaning:

USER-ID

The USER-ID column contains the login names to which the respective admission sets belong. If a login name longer than 8 characters is specified, the first 7 characters are output followed by an asterisk (*).

MAX-USER-LEVELS / MAX-ADM-LEVELS

The six columns under MAX-USER-LEVELS show the values specified by each of these FTAC users for their respective admission sets. The six columns under MAX-ADM-LEVELS contain the values set by the FTAC administrator. The lower of the two values determines whether or not the owner of this admission set may use the basic function specified.

The names of the basic functions are abbreviated as follows:

```
OBS = OUTBOUND-SEND
OBR = OUTBOUND-RECEIVE
IBS = INBOUND-SEND
IBR = INBOUND-RECEIVE
IBP = INBOUND-PROCESSING
IBF = INBOUND-FILE-MANAGEMENT
```

The values in the admission set have the following meaning:

0	The basic function is disabled.
10	The relevant basic function is enabled for all partner systems that have been authenticated in the local system.
90	The relevant basic function is enabled for partner systems whose names (->partner) are entered in the Transport Name Service, DNS / NIS or in the */etc/hosts* file (if an *ftstd* entry exists).
100	The inbound basic function is enabled for all partner systems.

*open*FT accepts and stores any whole number between 0 and 100. The admissions check is carried out, based on the next level down (0, 10, or 90).

An asterisk '*' after the value indicates that this entry was taken from the standard admission set and will automatically be modified if the value in the standard admission set is changed.

ATTR

PRIV in the column indicates the privileged admission set; *root* is the FTAC administrator. At the present time, there are no further attributes for the ATTR column.

5.19.1 CSV output format for an admission set

Column	Type	Values
UserId	String	Value enclosed in double quotes
UserMaxObs	Number	Value
UserMaxObsStd	String	*YES / *NO
UserMaxObr	Number	Value
UserMaxObrStd	String	*YES / *NO
UserMaxIbs	Number	Value
UserMaxIbsStd	String	*YES / *NO
UserMaxIbr	Number	Value
UserMaxIbrStd	String	*YES / *NO
UserMaxIbp	Number	Value
UserMaxIbpStd	String	*YES / *NO
UserMaxIbf	Number	Value
UserMaxIbfStd	String	*YES / *NO
AdmMaxObs	Number	Value
AdmMaxObsStd	String	*YES / *NO
AdmMaxObr	Number	Value
AdmMaxObrStd	String	*YES / *NO
AdmMaxIbs	Number	Value
AdmMaxIbsStd	String	*YES / *NO
AdmMaxIbr	Number	Value
AdmMaxIbrStd	String	*YES / *NO
AdmMaxIbp	Number	Value
AdmMaxIbpStd	String	*YES / *NO
AdmMaxIbf	Number	Value
AdmMaxIbfStd	String	*YES / *NO
Priv	String	*YES / *NO
Password	String	*YES / *NO

5.20 ftshwd - Display diagnostic information

With the *ftshwd* command, you can display diagnostic information.

The diagnostic documents are used by the Maintenance and Diagnostic Service of Fujitsu Siemens Computers for error diagnosis.

Format

ftshwd

Description

The command has no further switches. The following example shows the output for this command, and explains the meanings of the fields.

```
FTAC ADMINISTRATOR : root
NUMBER OF UADS     : 6
NUMBER OF PROFILES : 31
DATE     TIME    SSID  COMPONENT    LOCATION-ID       INFO
20031111 100921  FT    251/yfysequ  46/SwinsLwrite    ffffffff
20031111 100923  FTAC  39/yfslogg   1/WriteErr        ffffffff
```

FTAC-ADMINISTRATOR
: Login name of the FTAC administrator

NUMBER OF UADS (USER-ADMISSION-SET)
: Number of admission sets that deviate from the standard admission set

NUMBER OF PROFILES
: Number of available FT profiles

DATE
: Date when the error occurred

TIME
: Time at which the error occurred

SSID
: Subsystem ID; possible values: FT/FTAC

COMPONENT
: Module number/name

LOCATION-ID
: Function number/name

INFO
: Error code

5.21 ftshwe - Display FT profiles and admission sets from a file

ftshwe stands for "show environment", i.e. display FT profiles and admission sets from a file. Using *ftshwe*, the FTAC administrator can display FT profiles and admission sets that were saved using the *ftexpe* command.

Format

ftshwe -h |
<file name 1..512>
[-u=<user id 1..32>,...,<user id(100) 1..32>]
[-pr=<profile name 1..8>,...,<profile name(100) 1..8> | -pr=@n]
[-as=y | -as=n]
[-l] [-csv]

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

File name
file name specifies the file from which the FT profiles and admission sets are to be displayed.

-u=user id1[,user id2][,user id3]..
specifies the user IDs whose FT profiles and admission sets are to be displayed. You can specify up to 100 login names simultaneously.

If the specified user ID has no admission sets, only the standard admission set is displayed.

If you specify a non-existent login name for *user id1* , the current standard admission set is displayed.

-u not specified
all FT profiles and admission sets are displayed.

-pr=profile name1[,profile name2][,profile name3]... | -pr=@n
specifies the FT profiles to be displayed (up to 100).

@n for *profile name*
no FT profiles are displayed.

-pr not specified
: all FT profiles belonging to the user IDs specified in the -u parameter are displayed.

-as=y | -as=n
: specifies whether or not admission sets are to be displayed.

  y (default value)
  : all admission sets belonging to the login names specified in the -u parameter are displayed.

  n no admission sets are displayed.

-l specifies that you wish to see the contents of the selected FT profiles.

-l not specified
: displays only the names of the FT profiles. Markings also indicate whether or not an FT profile is privileged (*) and whether or not it is disabled (!).

-csv -csv specifies that the FT profiles and admission sets are to be output in CSV format. The values are output separated by semicolons. When -csv is specified, the output is always detailed (analogous to -l), regardless of whether or not -l is specified at the same time.

-csv not specified
: The FT profiles and admission sets are output in the standard format.

5.21.1 CSV output format of FT profiles and admission sets from a file

For a detailed description of this please refer to section “CSV output format for an FT profile” on page 146 and the section “CSV output format for an admission set” on page 130.

5.22 ftshwl - Display log records

With *ftshwl*, you can obtain information on all file transfer requests logged up to now by *open*FT.

As the administrator, you can display all log records in the system. The log records are stored in the file */var/openFT/instance/log/logdat* where *instance* means the name of the corresponding instance.

The log records are marked as FT and FTAC log records respectively, which means that you can determine the type of log record from the output.

For every request, there is a FTAC log record in which you can find the result of the FTAC admission check. If the check is positive and *open*FT has accepted the request, there is also a second *open*FT log record which indicates whether the request was successfully executed or why it was aborted.

If no options are specified, *open*FT outputs the current log record. If options are specified, *open*FT outputs all log records up to the time specified in the command in reverse chronological order, i.e. starting from the most recent record to the oldest record.

There are three types of output: short output, long output and CSV output (**C**omma **S**eparated **V**alue).

Output is written to standard output.

Format

```
ftshwl  [ -h] |
        [ <user id 1..32> | @a]
        [ -rg=[[[[yyyy]mm]dd]hhmm|#1..99999999|0..999|:0..999]  [-
              [[[[yyyy]mm]dd]hhmm|#1..99999999|0..999|:0..999]]]
        [ -rt=[t][c]]
        [ -ff=[t][m][r][d][a][C][D][M]]
        [ -ini=[l][r]]
        [ -pn=<partner 1..78>]
        [ -fn=<file name 1..512>]
        [ -nb=1..99999999 | -nb=@a]
        [ -rc=0..ffff | -rc=@f]
        [ -l ] [ -csv ]
```

Description

-h Displays the command syntax on the screen. Entries after the *-h* are ignored.

user id | @a
: is used to specify the login name(s) for which log records are to be displayed. As the administrator, you can specify any login name.

  @a for *user id*
  : FT or FTAC administrators can display the log records for all login names.

user id not specified
: Only the log records for the login name under which the command was entered are displayed.

-rg=[[[[yyyy]mm]dd]hhmm]-[[[[yyyy]mm]dd]hhmm]
: You can *-rg* to specify the start and/or end of a logging interval.

  [[[yyyy]mm]dd]hhmm
  : When specifying a time, a 4-digit specification is interpreted as the time expressed in hours and minutes, a 6-digit specification as the day (date) and time in hours and minutes, an 8-digit specification as the month, day, and time in hours and minutes, and a 12-digit specification as the year, month, day, and time in hours and minutes. The largest possible value that can be specified as the date is 20380120 (January 20, 2038).
    *open*FT then displays all the log records written during the specified time period. The older time is taken to be the start time and the earlier time as the end time. This means that the time period is viewed from the past towards the present.
    The optional data ([…]) is automatically replaced by current values. If one of the limiting values is omitted, the current time is taken to be the end time, and the start time is the time at which the first log record was written.

-rg=[[[yyyy]mm]dd]hhmm
: If the minus sign is missing, the range is the exact minute specified. The largest possible value that can be specified as the date is 20380120 (January 20, 2038). The optional data ([…]) is automatically replaced by current values.

-rg=[#1..99999999]-[#1..99999999]

-rg is used to specify the start and/or end of a range of log IDs.

#1..99999999

The selection of a log ID is indicated by the leading # character. *open*FT then displays all the log records which lie within the specified range. The older time is taken to be the start and the earlier time as the end. This means that you are looking from the past towards the present with regard to the time and the log IDs.

If one of the limiting values is omitted, the current ID is used as the end log ID, and the ID of the first log written is used as the start log ID.

-rg=#1..99999999

If the minus sign is omitted, the range is restricted to the specified log ID only.

-rg=0..999 [**-**0..999]

Here you specify with *-rg* a relative time period as a multiple of 24 hours (i.e. as a number of days). You can specify a 1- to 3-digit number. *open*FT then outputs all the log records that are older than this.
You are thus looking backward in time.

-rg=:0..999 [-:0..999]

Here you specify with *-rg* a relative time period in minutes. You can specify a 1- to 3-digit number. You have the following options in this case:

- Specifying *-rg=:0..999 -:0..999* will output all log records that lie within the specified time range with respect to the current time.
- Specifying *-rg=:0..999* will output the log records in the time span that starts with the current time and goes back into the past by the number of minutes you have specified.
- Specifying *-rg=-:0..999* will output the log records that lie outside of the specified time limit, meaning all records that are older than the time specified in minutes.

You are thus looking back in time.

-rg not specified

The range is not a selection criterion.

-rt=[t] [c]

Defines which type of log record is to be displayed.
Possible values are t, c, ct, or tc.

t The FT log records are displayed.
c The FTAC log records are displayed.
ct, tc The FT and FTAC log records are displayed.

-rt not specified
: The record type is not a selection criterion.

-ff=[t] [m] [r] [d] [a] [C] [D] [M]
: Defines the FT function for which log records are to be output. Possible values are: t, m, r, d, a, C, D and M or any combination of these values. The entries t, m, r, d, a, C, D and M are only valid for FTAC log records.

  t All log records for the function “transfer files” are output.

  m All log records for the function “modify file attributes” are output.

  r All log records for the function “read directories” are output.

  d All log records for the function “delete files” are output.

  a All log records for the function “read file attributes” are output.

  C All log records for the function “Create directory” are output.

  D All log records for the function “Delete directory” are output.

  M All log records for the function “Modify directory” are output.

-ff not specified
: The FT function is not a selection criterion.

-ini=[l] [r]
: Defines the initiator for which log records are to be output. Possible values are: l, r, lr, rl.

  l Only log records belonging to file transfer functions issued locally are output.

  r Only log records belonging to file transfer and file management functions issued remotely are output.

  lr, rl The log records belonging to file transfer and file management functions issued locally and remotely are output.

-ini not specified
: The initiator is not a selection criterion.

-pn=partner
: Defines the partner system to which the log records are to be output.

-pn not specified
: The partner system is not a selection criterion.

-fn=file name
Defines the file to which the log records are to be output.

-fn not specified
The file name is not a selection criterion.

-nb=number | @a
Defines the number of log records to be output.

@a for *number*
All log records are output.

-nb not specified
If *-rg* has also been specified, *-nb* is replaced by the value *-nb=@a*.

If *-rg* is also not specified, *-nb* is replaced by the value *-nb=1*.

-rc=0..ffff | @f
Defines the reason code as a selection criterion for log record output.

0 .. ffff
All log records with a specified reason code are output.

@f All log records with reason codes other than 0000 are output. This criterion yields a list of log records for all requests terminated with error messages.

-rc not specified
The reason code is not a selection criterion.

-l Defines that the log records are to be output in long form.

-l not specified
The log records are output in short form.

-csv You can use *-csv* to specify that the log records are to be output in the CSV format. The values in the output are separated by semicolons. If *-csv* is specified, output is always in long form (analogous to *-l*) regardless of whether or not *-l* has also been specified.

-csv not specified
The log records are output in the standard format.

Examples

1. All log records that are more than two days (48 hours) old are output:

   ```
   ftshwl ... -rg=2
   ```

2. All log records that are more than 15 minutes old but less than 30 minutes old are output:

   ```
   ftshwl ... rg=:15-:30
   ```

3. All log records that are less than 30 minutes old (as of the current time) are output:

   ```
   ftshwl ... -rg=:30
   ```

4. All log records that are more than 30 minutes old are output:

   ```
   ftshwl ... -rg=-:30
   ```

5.22.1 Description of log record output

Log records can be displayed using the graphical user interface or by using the *ftshwl* command. You can choose between a short overview, detailed information or, if further processing is to be performed with external programs, output in the CSV format.

The log records are identified by log IDs. The log IDs are assigned in ascending order, but for technical reasons the numbering of the log IDs is not always contiguous (i.e. there may be gaps).

The log record output and the reason codes of the logging function are described in the User Guide.

5.22.1.1 Logging requests with preprocessing/postprocessing

For security reasons, only the first 32 characters (or 42 characters in the case of *ftexecsv* preprocessing) of a preprocessing or postprocessing command are transferred to the log record. By arranging the call parameters appropriately or by inserting blanks, you can influence which command parameters do not appear in the log.

5.23 ftshwp - Display FT profiles

tshwp stands for "show profile" and allows you to obtain information about FT profiles. In short form, it displays the names of the selected FT profiles, as well as the following information:

– whether or not the FT profile is privileged asterisk (*) before the profile name
– whether or not the transfer admission is disabled exclamation mark (!) before the profile name.

As the FTAC administrator, you may obtain information about all FT profiles in the system.

Format

ftshwp -h |
[<profile name 1..8>]
[-s=[<transfer admission 8..16> | @a | @n][,<user id 1..32> | @a]]
[-l] [-csv]

Description

-h Displays the command syntax on the screen. Entries after the are ignored.

profile name
Is the name of the FT profile you wish to see.

profile name not specified
Profile name is not used as a criterion for selecting the FT profile to be displayed. If you do not specify the profile with -s (see below), FTAC will display information on all of your FT profiles.

-s=[transfer admission | @a | @n][,user id | @a]
Is used to specify criteria for selecting the FT profiles to be displayed.

Transfer admission
Is the transfer admission of the FT profile to be displayed.

@a for *transfer admission*
Displays information either on the FT profile specified with *profile name* (see above) or (if no *profile name* was specified) on all FT profiles.

As the FTAC administrator, you can specify *@a* if you want to obtain information on FT profiles belonging to other login names, since even you should not know the transfer admission.

@n for *transfer admission*
As the FTAC administrator, you can specify *@n* if you want to obtain information on FT profiles belonging to other login names which do not have defined transfer admissions.

transfer admission not specified
causes FTAC to query the transfer admission on the screen after the command is entered. Your entry is not displayed to prevent unauthorized persons from seeing the transfer admission. To exclude the possibility of typing errors, the program prompts you to enter the transfer admission a second time. If you just press ↵, this has the same effect as specifying *@a*.

,user id
As the FTAC administrator, you can specify any login name here.

@a for *user id*
As the FTAC administrator, you can obtain information on the FT profiles of all login names.

user id not specified
displays only profiles belonging to the user's own login name, regardless of who issues the command.

-s not specified
if no profile name is specified, displays all the FT profiles belonging to the login name under which the *ftshwp* command is issued. Otherwise, displays information on the FT profile with the specified name.

-l displays the contents of the selected FT profiles.

In long form, the entire contents of the selected FT profiles are displayed. The USER-ADM parameter contains the following information:
– the login name for which it is valid
– whether or not it is valid for a specific password of the login name
– whether or not it is valid for any password of the login name
– whether or not it has an undefined password and is thus disabled.

USER-ADM=	**Meaning**
(user ID,,OWN)	Profile is valid for all passwords of the login name.
(user ID,,YES)	The profile is valid only for a specific password of the login name (specified in *-ua=user ID, password* with an *ftcrep* or *ftmodp* command). The profile is deactivated (not disabled) if the password is changed. You can activate it again, for example, by resetting the password.
(user ID,, NOT-SPECIFIED)	The FTAC administrator created or modified the FT profile knowing only the login name. As a result, the profile was disabled. You must enable the profile with *ftmodp* and the *-v=y* parameter.

If an FT profile is disabled, the *TRANS-ADM* parameter indicates the reasons why the profile was disabled. The following table shows the possible parameter values, as well as their meanings:

TRANS-ADM=	**Possible cause and action**
NOT-SPECIFIED	The FTAC administrator created the FT profile without transfer admission, or the FTAC user did not specify transfer admission. Measure: specify transfer admission
DUPLICATED	An attempt was made to create an FT profile with the same transfer admission. Measure: specify new transfer admission
LOCKED (by_adm)	The FTAC administrator modified the FT profile by login name only. The transfer admission remained unchanged but was disabled. Measure: enable the profile using the *ftmodp* command and the *-v=y* parameter
LOCKED (by_import)	The FT profile was created using the *ftimpe* command. The transfer admission remains unchanged, but is marked as disabled. Measure: enable the profile using the *ftmodp* command and the *-v=y* parameter.

TRANS-ADM=	Possible cause and action
LOCKED (by_user)	The FTAC user disabled his/her own FT profile. Measure: enable profile using the *ftmodp* command and the *-v=y* parameter.
EXPIRED	The time up to which the transfer admission can be used has expired. Measure: enable profile using the *ftmodp* command and the *-d* parameter, by removing the temporal restriction using the *-d* entry and defining a new time span with *-d=date*.

ftshwp does not, however, provide a means of displaying a transfer admission. If you have forgotten a transfer admission, you have to define a new one using *ftmodp*.

-l not specified
: displays only the names of your FT profiles. Markings also indicate whether or not an FT profile is privileged (*) and whether or not it is disabled (!).

-csv You can use *-csv* to specify that the FT profiles are to be output in the CSV format. The values in the output are separated by semicolons. If *-csv* is specified, output is always in long form (analogous to *-l*) regardless of whether or not *-l* has also been specified.

-csv not specified
: The FT profiles are output in the standard format.

5.23.1 CSV output format for an FT profile

Column	Type	Value
ProfName	String	Value enclosed in double quotes
Priv	String	*YES / *NO
TransAdm	String	*NSPEC / *SECRET
Duplicated	String	*YES / *NO
LockedByImport	String	*YES / *NO
LockedByAdm	String	*YES / *NO
LockedByUser	String	*YES / *NO
Expired	String	*YES / *NO
ExpDate	yyyy-mm-dd	Value / *NRES
Usage	String	*PUBLIC / *PRIVATE / *NSPEC
IgnObs	String	*YES / *NO
IgnObr	String	*YES / *NO
IgnIbs	String	*YES / *NO
IgnIbr	String	*YES / *NO
IgnIbp	String	*YES / *NO
IgnIbf	String	*YES / *NO
Initiator	String	*LOC / *REM / *NRES
TransDir	String	*FROM / *TO / *NRES
MaxPartLev	Number	Value / *NRES
Partners	String	One or more FT partners, delimited by commas and enclosed in double quotes / *NRES
FileName	String	Value enclosed in double quotes / *NRES
Library	String	*YES / *NO / *NRES / Value enclosed in double quotes
FileNamePrefix	String	*YES / *NO
ElemName	String	Value enclosed in double quotes / *NRES / *NONE

Column	Type	Value
ElemPrefix	String	*YES / *NO
ElemVersion	String	Value enclosed in double quotes / *STD / *NONE / *NRES
ElemType	String	Value enclosed in double quotes / *NRES / *NONE
FilePass	String	*YES / *NRES / *NONE
Write	String	*NEW / *EXT / *REPL / *NRES
UserAdmId	String	Value enclosed in double quotes
UserAdmAcc	String	Value enclosed in double quotes / *NSPEC / *NRES
UserAdmPass	String	*OWN / *NSPEC / *NONE / *YES
ProcAdmId	String	Value enclosed in double quotes / *NRES / *SAME
ProcAdmAcc	String	Value enclosed in double quotes / *NRES / *SAME
ProcAdmPass	String	*NONE / *YES / *NRES /*SAME
SuccProc	String	Value enclosed in double quotes / *NONE / *NRES / *EXPANSION
SuccPrefix	String	Value enclosed in double quotes / *NONE
SuccSuffix	String	Value enclosed in double quotes / *NONE
FailProc	String	Value enclosed in double quotes / *NONE / *NRES / *EXPANSION
FailPrefix	String	Value enclosed in double quotes / *NONE
FailSuffix	String	Value enclosed in double quotes / *NONE
TransFile	String	*ALLOWED / *NOT-ALLOWED
ModFileAttr	String	*ALLOWED / *NOT-ALLOWED
ReadDir	String	*ALLOWED / *NOT-ALLOWED
FileProc	String	*ALLOWED / *NOT-ALLOWED
Text	String	Value enclosed in double quotes/ *NONE
DataEnc	String	*NRES / *YES / *NO

5.24 ftupdi - Update the instance directory

Using *ftupdi*, you can update an instance file tree that was made using *open*FT V8.0 so that it can continue to be used with *open*FT V8.1. The settings of the operational parameters, FTAC admission sets, FTAC admissions profiles and log records are retained.

Any interrupted requests for this instance which are still present will be lost.

Format

ftupdi -h |
<directory 1..128>

Description

-h displays the command syntax on the screen. Any entries after *-h* are ignored.

<directory 1..128>
Here, you enter the directory which contains the instance file tree of the instance to be updated.

Messages of the ftupdi command

If *ftupdi* could not be carried out as specified, an explanatory message is displayed; the exit code will then be “not equal to zero.”

Example

The FT administrator wants to update the directory of the instance *hugo*.

```
ftupdi /var/openFT/.hugo
```

5.25 ftupdk - Update public keys

Using *ftupdk*, you can update the public key files of existing key pair sets.

For example, you can use it to insert updated comments from the *syspkf.comment* file into existing public key files or replace accidentally deleted public key files of a key pair set.

Format

ftupdk [-h]

Description

-h displays the command syntax on the screen. Any entries after *-h* are ignored.

Example

The name of the FT administrator is to be imported into the public key files. First, the file *syspkf.comment* in the directory */var/openFT/instanz/config* is edited using an editor.

The file might, for example, contain only the following line:

```
FT administrator: John Smith, Tel. 12345
```

The command is:

```
ftupdk
```

The command is executed without an error message. Following this, the information will be placed at the beginning of all *syspkf...* public key files as a comment line.

5.26 install.ftam - Install *open*FT-FTAM

The *install.ftam* command allows you to install and uninstall *open*FT-FTAM. Installation is only permitted if you have an *open*FT-FTAM license.

The *install.ftam* script is located in the */opt/openFT/bin/ftbin* directory.

Format

install.ftam –h | -i | -d

Description

-h Displays the command syntax. Anything specified after *-h* is ignored.

-i *open*FT-FTAM is installed.

-d *open*FT-FTAM is uninstalled.

6 What if ...

... the BS2000 system cannot be accessed

Depending on which partner has the initiative, you should check the following points.

UNIX to BS2000:

If your local system in BS2000 is unknown, enter the command *add-ft-partner* in BS2000.

If you receive the message “Remote system not available”, check whether one of the following reasons is the cause:

– Resource bottleneck in the remote system
– Remote FT system is not started
– BCIN is missing
– no network connection (for a TCP/IP connection, check the connection with the command *ping*, for example)
– Name server entry

BS2000 to UNIX:

If neccessary, check whether one of the following reasons is the cause in the BS2000 system:

– BCMAP entry is missing or invalid
– BCIN is missing
– Partner entry (*add-ft-partner*) refers to a wrong BCAM name
– BCACT is missing. Test the availability of a partner with a synchronous command (e.g *SHOW-REM-FILE-ATTRIBUTE*)

... the name of the partner is missing in the log records

Enter the partner in the TNS, in the DNS or */etc/hosts*.

... the logging function cannot be called or the log file is corrupted

The only remedy here, is to terminate *open*FT (*fta -t*) and delete the log file as follows:

```
rm /var/openFT/instance/log/logdat.idx
```

However, this means that you lose all log records. Here *instance* means the name of the corresponding instance.

... You are not given a free transport connection for an ncopy request

check you TNS entries.

... the *open*FT message “Remote transfer admission invalid” appears

For reasons of data security, this message does not differentiate between the various possible reasons for the rejection on the initiator side. This information is only available via the *open*FT logging of the responder system.

... Do requests still remain in the “WAIT” state?

Using *fti -l,* you can obtain information on the exact cause:

RAUTH
: Authentication of the partner in the local system has failed. Solution: Store the current, public key of the partner system in the directory *syskey* of the local *open*FT instance and name the key file using the name of the instance ID of the partner system, in lowercase.

LAUTH
: Authentication of the local system in the partner has failed. Solution: Transmit the current, public key of the local *open*FT instance to the partner and store it there appropriately.

NOKEY
: One of the two systems engaged in the transfer does not support encryption. Check to see whether at least one key pair set exists in the local system.

You can find other possibilities in the description of the command *fti* in the user’s guide.

.. Deleting a request in the *open*FT Explorer takes an unusually long time (about 1 minute)

This may mean

– that a request was issued to send a mail when the request to be deleted is finished

– and that the mail function of the UNIX system takes about 1 minute to send a mail due to a configuration problem.

Solution:

Do not ask for a mail to be sent when the request is finished, i.e. specify the *-m=n* option for the *ft* command. Requests that are started in the *open*FT Explorer never require a mail to be sent when finished.

Performance note

The RFC1006 protocol is far more efficient than communicating via LANINET. In UNIX, the choice of which protocol is to be used is made via the TNS entries. In BS2000, the type of the global BCMAP entry determines the protocol type: if the PTSEL-I entry exists, RFC1006 is used.

6.1 Actions in the event of an error

If, in spite of precautions, an error occurs which neither the FTAC administrator nor the system administrator can rectify, please contact your local Fujitsu Siemens Computers contact partner. In order to simplify error diagnosis, you should provide the following documents:

– an exact description of the error situation and information as to whether the error is reproducible;

– the version number of the file transfer product in the remote computer;

– diagnostic information (which is created with the FT command *ftshwd*);

– if available, the FTAC and FT log records (which are output with the FT command *ftshwl ...*);

– if available, the *open*FT trace file;

– for errors related to a specific FT profile a printout of the profile (*ftshwp␣profilename␣-l*) and a printout of the admission sets (*ftshwa␣@a*).

– version of the operating system

– version of the communication system (CMX)

– if necessary, the process tables (ps command)

7 Diagnosis

This chapter describes how you can create and evaluate trace files.

Further diagnostic information can be obtained with the help of the command “ftshwd - Display diagnostic information” on page 131.

At the end of this chapter you will find code tables with which you can diagnose code conversion errors.

7.1 Trace files

You can switch trace mode on or off for the purposes of error diagnosis, using
– the *fta -n/-f* command
– or the graphical interface.

When trace mode is switched on, diagnostic data is written to trace files which are located in the directory */var/openFT/std/traces* or, if the traces were created by another *open*FT instance, in the subdirectory *traces* residing in the corresponding instance directory. When you have finished diagnosis, you should deactivate the trace mode for reasons of performance. The trace files can become infinitely large, since they are not cyclically overwritten.

The trace file names are based on the following concept:

For requests involving *open*FT partners, *open*FT creates file names with the following format: **T**tthhmmssxxxxx. A separate file is created for each process.

For requests involving FTAM partners, *open*FT makes a distinction between synchronous (*ncopy*, *ftshw*, *ftdel*, *ftmod*) and asynchronous (*ft*) requests.
Synchronous requests generate file names with the format: **N**ddhhmmssxxxxx
Asynchronous requests generate file names with the format: **S**nnddhhmmss.ii

The file names contain the time at which *open*FT created the files:

tt:	day on which openFT created the file
hhmmss	time in hours, minutes, seconds
xxxxx	5-digit process identification
nntt	month and day
ii	ascending number of server processes

If *open*FT is started, the trace file is created immediately after trace mode is switched on; if *open*FT is not started, then it is created after the next activation. The trace files are updated until the next time trace mode is switched off.

When linked with *open*FT partners, trace files can be evaluated with the utility routine *fttrace* (*open*FT: */opt/bin/fttrace*).
With FTAM partners, trace files can be evaluated with the */opt/openFT/bin/ftbin/step* utility routine.

7.1.1 Evaluating trace files for *open*FT partner systems

With *open*FT partners, trace files are evaluated with the *fttrace* utility program as follows:

fttrace[␣-**d**][␣-**s**[=]security requirements]␣file1[␣file2]...

Only one of the following options may be specified before the desired trace file(s). If no option is specified, *-s=m* is used.

-**d** no analysis, i.e. dump output of the SOP and SOY protocol elements

-**s**=security requirement
specifies the data in the converted file to be displayed. Possible values are n, l, m and h.

- **n** no security requirement
- **l** no passwords are displayed
- **m** no login names, account numbers, passwords, and follow-up processing commands are displayed
- **h** no login names, account numbers, passwords, follow-up processing commands, or file names are displayed

file1[␣file2]...
Name of the trace file(s). The file names must be specified in full. Wildcards are permitted.

7.1.2 Defining the range of trace files for FTAM partner systems

Using the diagnostic program *ossd*, you can modify the range of FTAM trace records, e.g. in order to display the contents of a transferred file. This is achieved as follows:

1. Terminate *open*FT.
2. Switch on the *open*FT trace.
3. Change to the appropriate directory, as described below:
   - for requests issued using the *ft* command, change to the FT directory
   - for requests issued using the *ncopy* command, change to the directory in which the *ncopy* command was invoked

   In the current directory, *ossd* creates a file called *SYOSS.TRO*, which contains the options of the *ossd* call described below and defines the trace range.
4. Call the *ossd* program as follows*:*

   /opt/openFT/bin/ftbin/ossd␣**-n**␣file name␣
   [[mode]␣[**noev**]␣[options]
   [[maxuserdata]/[maxsdata]/[maxstypeddata]]]

   -n␣file name
   Name of the first trace file to be generated.

   mode
   Mode in which the trace file is to be opened. Possible values are *new* or *ext*. With *new*, a new trace file is opened (default value). With *ext*, the file is extended, assuming it already exists.

   selected trace
   Specification of the trace to be activated. You can specify *user* (user trace), *serv* (service trace), and/or prot (protocol trace). Several specifications can be combined in the specified order using the + character.

   noev
   Non-specific OSS events (NOEVENT) are also recorded.

   maxuserdata
   Maximum number of bytes of data to be recorded not of types S-DATA and S-TYPED-DATA or *unlim* if this is unlimited.

maxsdata
: Maximum number of bytes of data of type S-DATA to be recorded, or *unlim* if this is unlimited.

maxstypeddata
: Maximum number of bytes of data of type S-TYPED-DATA to be recorded, or *unlim* if this is unlimited.

5. Start *open*FT.
6. You can now evaluate the *open*FT trace files as described below.

7.1.3 Evaluating trace files for FTAM partner systems

With FTAM partners, trace files are evaluated with the *step* utility as follows:

/opt/openFT/bin/ftbin/step[␣**-h**][␣**-d**][␣**-l**=nnn[k]]
[␣**-s**[=]security requirements]
[␣**-ps**=protocol layer][␣**-cref**=n]
[␣**-f**=start time][␣**-t**=end time]
␣file1[␣file2]...

-**h** Outputs the command syntax on the screen. Specifications following the *-h* are ignored.

-**d** No analysis of user data from session PDUs.

-**l=**nnn[k]
: Maximum length of the dumps in [K]bytes, rounded off to multiples of 16. The length is shown in the message *output limit reached*.

-**s**=security requirement
: Indicates which data are to be shown in the edited file. The options are *n*, *l*, *m* and *h*.

  n No security requirement

  l No passwords are displayed

  m (Default)
  : No login names, account numbers, passwords are displayed

  h No login names, account numbers, passwords and file names are displayed

-**ps=**protocol layer

The protocol layer for which events or PDUs (Protocol Data Units) are to be displayed. The options are *t*, *s*, *p*, *a* and *F*.

t Transport events (without the transport data)

s Session events, i.e. with transport events and transport data

p Presentation events

a ACSE events

F FTAM events

Trace records containing information on abnormal protocol events - for example *diagnostics* in an FTAM-PDU - are always output.

ps not specified

All events are output.

-**cref=**n

The trace record to be edited. *n* is the number of the connection reference or session reference. This number can be eight digits long and can be taken from an edited trace file.

-**f=**starttime

-f sets a time of day. All trace files written as of this time are evaluated. The format for *start time* is *hh*:[*mm*:[*ss*]].

hh hours

mm minutes

mm not specified

The minutes counter is set to 00.

ss seconds

ss not specified

The seconds counter is set to 00.

f not specified

The default start time is 00:00:00.

-t=finish time

-*t* sets a time of day. All trace files written as up to this time are evaluated. The format for *finish time hh*:[*mm*:[*ss*]].

hh hours

mm minutes

mm not specified
The minutes counter is set to 00.

ss seconds

ss not specified
The seconds counter is set to 00.

t not specified
The default finish time is 00:00:00.

file1[␣file2]...

Name of the trace file(s). The file names must be specified in full. Wildcards are permitted.

The *step* utility evaluates trace files that contain a session service trace. The result is a printable file.
If the -*d* switch was not set when the trace utility was started, the program attempts to interpret the protocols (see -*ps*) in the user data of the session PDUs.

7.2 Code tables

7.2.1 Code conversion table EBCDIC.DF.04-x to ISO8859-x

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	02	03	80	09	81	7F	82	83	84	0B	0C	0D	0E	0F
1	10	11	12	13	85	86	08	87	18	19	88	89	1C	1D	1E	1F
2	8A	8B	8C	8D	8E	0A	17	1B	8F	90	91	92	93	05	06	07
3	94	95	16	96	97	98	99	04	9A	9B	9C	9D	14	15	9E	1A
4	20	A0	E2	E4	E0	E1	E3	E5	E7	F1	60	2E	3C	28	2B	7C
5	26	E9	EA	EB	E8	ED	EE	EF	EC	DF	21	24	2A	29	3B	9F
6	2D	2F	C2	C4	C0	C1	C3	C5	C7	D1	5E	2C	25	5F	3E	3F
7	F8	C9	CA	CB	C8	CD	CE	CF	CC	A8	3A	23	40	27	3D	22
8	D8	61	62	63	64	65	66	67	68	69	AB	BB	F0	FD	FE	B1
9	B0	6A	6B	6C	6D	6E	6F	70	71	72	AA	BA	E6	B8	C6	A4
A	B5	AF	73	74	75	76	77	78	79	7A	A1	BF	D0	DD	DE	AE
B	A2	A3	A5	B7	A9	A7	B6	BC	BD	BE	AC	5B	5C	5D	B4	D7
C	F9	41	42	43	44	45	46	47	48	49	AD	F4	F6	F2	F3	F5
D	A6	4A	4B	4C	4D	4E	4F	50	51	52	B9	FB	FC	DB	FA	FF
E	D9	F7	53	54	55	56	57	58	59	5A	B2	D4	D6	D2	D3	D5
F	30	31	32	33	34	35	36	37	38	39	B3	7B	DC	7D	DA	7E

Code conversion table EBCDIC.DF.04-x to ISO8859-x

7.2.2 Code conversion table ISO8859-x to EBCDIC.DF.04-x

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	02	03	37	2D	2E	2F	16	05	25	0B	0C	0D	0E	0F
1	10	11	12	13	3C	3D	32	26	18	19	3F	27	1C	1D	1E	1F
2	40	5A	7F	7B	5B	6C	50	7D	4D	5D	5C	4E	6B	60	4B	61
3	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	7A	5E	4C	7E	6E	6F
4	7C	C1	C2	C3	C4	C5	C6	C7	C8	C9	D1	D2	D3	D4	D5	D6
5	D7	D8	D9	E2	E3	E4	E5	E6	E7	E8	E9	BB	BC	BD	6A	6D
6	4A	81	82	83	84	85	86	87	88	89	91	92	93	94	95	96
7	97	98	99	A2	A3	A4	A5	A6	A7	A8	A9	FB	4F	FD	FF	07
8	04	06	08	09	0A	14	15	17	1A	1B	20	21	22	23	24	28
9	29	2A	2B	2C	30	31	33	34	35	36	38	39	3A	3B	3E	5F
A	41	AA	B0	B1	9F	B2	D0	B5	79	B4	9A	8A	BA	CA	AF	A1
B	90	8F	EA	FA	BE	A0	B6	B3	9D	DA	9B	8B	B7	B8	B9	AB
C	64	65	62	66	63	67	9E	68	74	71	72	73	78	75	76	77
D	AC	69	ED	EE	EB	EF	EC	BF	80	E0	FE	DD	FC	AD	AE	59
E	44	45	42	46	43	47	9C	48	54	51	52	53	58	55	56	57
F	8C	49	CD	CE	CB	CF	CC	E1	70	C0	DE	DB	DC	8D	8E	DF

Code conversion table ISO8859-x to EBCDIC.DF.04-x

7.2.3 Code table EBCDIC.DF.04

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0					SP	&	-	¢	Ø	°	µ	¢	ù	¦	Ù	0
1					NBSP	é	/	É	a	j	‾	£	A	J	³	1
2					â	ê	Â	Ê	b	k	s	¥	B	K	S	2
3					ä	ë	Ä	Ë	c	l	t	•	C	L	T	3
4					à	è	À	È	d	m	u	©	D	M	U	4
5					á	í	Á	Í	e	n	v	§	E	N	V	5
6					ã	î	Ã	Î	f	o	w	¶	F	O	W	6
7					å	ï	Å	Ï	g	p	x	¼	G	P	X	7
8					ç	ì	Ç	Ì	h	q	y	½	H	Q	Y	8
9					ñ	ß	Ñ	¨	i	r	z	¾	I	R	Z	9
A					‘	!	^	:	<<	ª	;	¬	SHY	¹	²	³
B					.	$	,	#	>>	º	¿	[	ô	û	Ô	{
C					<	*	%	@	ð	æ	Ð	\	ö	ü	Ö	Ü
D					(	)	_	‘	ý	,	Ý	]	ò	Û	Ò	}
E					+	;	>	=	Þ	Æ	þ	´	ó	ú	Ó	Ú
F					|		?	“	±	¤	®	x	õ	ÿ	Õ	~

Code table EBCDIC.DF.04 (character set corresponding to ISO 8859-1)

7.2.4 Code table ISO 8859-1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0			SP	0	@	P	`	p			NBSP	°	À	Ð	à	ð
1			!	1	A	Q	a	q			¡	±	Á	Ñ	á	ñ
2			"	2	B	R	b	r			¢	^{2}	Â	Ò	â	ò
3			#	3	C	S	c	s			£	^{3}	Ã	Ó	ã	ó
4			$	4	D	T	d	t			¤	´	Ä	Ô	ä	ô
5			%	5	E	U	e	u			¥	m	Å	Õ	å	õ
6			&	6	F	V	f	v			¦	¶	Æ	Ö	æ	ö
7			´	7	G	W	g	w			§	•	Ç	x	ç	³
8			(	8	H	X	h	x			"	,	È	Ø	è	ø
9			)	9	I	Y	i	y			©	^{1}	É	Ù	é	ù
A			*	:	J	Z	j	z			ª	º	Ë	Ú	ê	ú
B			+	;	K	[	k	{			«	»	Ê	Û	ë	û
C			,	<	L	\	l	|			¬	$^1/_4$	Ì	Ü	ì	ü
D			-	=	M	]	m	}			SHY	$^1/_2$	Í	Ý	í	ý
E			.	>	N	^	n	~			®	$^3/_4$	Î	Þ	î	þ
F			/	?	O	-	o				¯	¿	Ï	b	ï	ÿ

Code table ISO 8859-1

8 Appendix

8.1 Important CMX commands

This section contains a short description of the most important CMX commands needed for the *open*FT configuration. You will find detailed information in the manual „CMX Operation and Administration“.

tnsxcom - Create the TS directory

With the *tnsxcom* command you can transfer files in the *tnsxfrm* format to TS directories. You can set different modes for functions such as the syntax check, update or recreating the TS directory.

The command has the following syntax (abbreviated):

tnsxcom [**-l -s -S -u -i**] [file]

The options have the following meanings:

-l LOAD mode
tnsxcom takes the entries our of the file *file* one at a time and fills the (previously empty) TS directory with the syntactically correct entries.

-s CHECK mode
tnsxcom only applies the syntax check to the file *file* and records any possible syntax errors. The TS directory is not changed.

-S CHECK-UPD mode
Like for the *-s* option, the syntax check is run on the entire file *file* in the first run. If no syntax errors are found, then *tnsxcom* updates the TS directory in a second run.

-u UPDATE mode
tnsxcom takes the entries our of the file *file* one at a time and merges the syntactically correct entries in the TS directory. Missing entries are created and existing entries are updated during this process.

-i INTERAKTIVE mode
tnsxcom reads entries in the *tnsxfrm* format from stdin after it has indicated it is ready to receive input by outputting a prompt and merges them in the TS directory. Missing entries are created and existing entries are updated during this process.

file The name of the file with the entries in the *tnsxfrm* format that are to be evaluated when the *-l*, *-s*, *-S* or *-u* options are specified. You can specify more than one file.

Example

The following call transfers the entries in the file *input.dir* to the current TS directory:

```
tnsxcom -S input.dir
```

tnsxprop - Output properties of TS applications

tnsxprop outputs all values of all properties that are located in a TS directory for the specified TS applications to stdout in a printable format.

You can specify in which format the properties are to be output using the first parameter.

The TS applications are determined by the parameter values for *name*. The parameter values for *name* can also be passed to *tnsxprop* from the file *file*. If no data was specified for *name* or *file*, then *tnsxprop* prepares the properties of all TS applications in the TS directory in the specified format.

The command has the following syntax (abbreviated):

tnsxprop [**-S** | **-h**] [**-f** file] [name ...]

-S This is the default setting. This option can be used to output the properties in symbolic form in the *tnsxfrm* format.

-h This option can be used to prepare the properties in hexadecimal form. The output is a string of hexadecimal digits together with the corresponding bit representation in which the lowest valued bit is located on the far right.

-f file

You specify for *file* the name of a file that contains the GLOBAL NAMES of the TS application whose properties are to be queried. The GLOBAL NAMES are to be specified as described under *name*.

name The GLOBAL NAME of the TS application in the TS directory is to be specified as follows for *name*:

NP5.NP4,NP3.NP2.NP1

The individual NP*i's* are the name attributes of the GLOBAL NAME.

NP5 is name attribute [5], i.e. it is the part of the name of the lowest hierarchy level. NP1 is name attribute [1], i.e. it is the part of the name of the highest hierarchy level. The name attributes are to be specified in ascending order hierarchically from left to right.

If one of the name attributes for a GLOBAL NAME does not contain data (e.g. NP4) and a name attribute of a higher level follows this name attribute (e.g. NP3), then only the separator (.) is to be specified for the name attribute that does not contain data. A series of separators at the end of the value of *name* does not have to be specified.

If the name attributes contain special characters whose special meaning would cause the syntax to take on multiple meanings, then these special characters must be delimited using the backslash (\). When in doubt, you should delimit every special character. Superfluous characters are ignored by *tnsxprop*.

If you specify an asterisk (*) for a name attribute, then *tnsxprop* returns the properties of all TS applications that match all other name attributes specified in *name* (TS_RESTRICTED filter mode).

Examples

1. The properties of the TS application that only has name attribute [5] set to the value *example_1* are to be output in hexadecimal form:

   ```
   tnsxprop -h example_1
   ```

2. The properties of the TS application that only has name attribute [5] set to the value *example_1* are to be output in symbolic form:

   ```
   tnsxprop example_1
   ```

3. The properties of all TS applications are to be output to a file *tns*:

   ```
   tnsxprop > tns
   ```

8.2 *open*FT in a UNIX Cluster

Software requirements

The same version of *open*FT must be installed on all nodes of the cluster. In addition, the following communications software is required:

SUN Solaris (Sparc)	CMX version 5.1E50 and later
Reliant UNIX	CMX version 5.1E40 and later
all platforms	PCMX version 4.1A10 and later

On SUN and Reliant UNIX, TNS inputs are only allowed to contain TCP/IP components. An input file for the *tnsxcom* command could look like the following:

```
$FJAM      DEL

$FJAM\
   TSEL    RFC1006  T'$FJAM'    ; input for TCP/IP-RFC1006
   TSEL    LANINET  A'1100'     ; input for TCP/IP

$FJAM_OUTBOUND      DEL

$FJAM_OUTBOUND\
   TSEL    RFC1006  T'$FJAMOUT' ; input for TCP/IP-RFC1006
   TSEL    LANINET  A'1101'     ; input for TCP/IP

$FTAM      DEL

$FTAM
   PSEL    V''                  ; blank presentation selector
   SSEL    V''                  ; blank session selector
   TSEL    RFC1006  T'$FTAM'    ; input for TCP/IP-RFC1006
   TSEL    LANINET  A'4800'     ; input for TCP/IP
```

During this, the existing inputs in the TNS are overwritten by *tnsxcom*.

Example 1: a fail-safe instance

The Unix cluster TREE (IP-address 123.25.10.12) consists of the two computers MAPLE (IP-address 123.25.10.1) and BEECH (IP-address 123.25.10.2). The failure management concept allows TREE to run either on MAPLE or BEECH. Only one openFT instance is fail-safe in this case.

Configure the cluster in such a way that a disk is always available. In this example, it is the directory */openFT*.

Required steps for the computer MAPLE

1. Install *open*FT version 8.1 for Unix (including the add-on products *open*FT CR and *open*FT FTAM, if necessary)
2. Deactivate *open*FT:

   ```
   fta -t
   ```

3. Adapt the $FJAM and $FJAM_OUTBOUND TNS inputs to Sun and Reliant Unix. They may only contain RFC1006 and LANINET inputs, see above.
4. Set the address for the instance *std*:

   ```
   ftmodi std -addr=MAPLE
   ```

5. Activate *open*FT on the instance *std* and set the ID, if this did occur automatically during installation:

   ```
   . ftseti std; fta -s [-id=MAPLE.FOREST.NET]
   ```

6. Mount the disk */openFT* on MAPLE.
7. Create the new instance *cluster* and check it. The directory */openFT* must exist, whereas the directory */openFT/cluster* must not exist:

   ```
   ftcrei cluster /openFT/cluster -addr=TREE.FOREST.NET
   ftshwi @a -l
   ```

8. If authentication is to be used in the instance *cluster*, then public keys from the partner systems must be stored in the directory */openFT/cluster/syskey*, or the public key from the directory */openFT/cluster/config* must be made available to the partner systems.
9. Deactivate the instance *cluster*:

   ```
   ftseti std; ftdeli cluster
   ```

Required steps on for the computer BEECH

1. Install *open*FT V8.1 for Unix (including the add-on products *open*FT CR and *open*FT FTAM, if necessary)
2. Deactivate *open*FT:

   ```
   fta -t
   ```

3. Adapt the $FJAM and $FJAM_OUTBOUND TNS inputs to Sun and Reliant Unix. They may only contain RFC1006 and LANINET inputs, see above.
4. Set the address of the instance *std*:

   ```
   ftmodi std -addr=BEECH
   ```

5. Activate *open*FT on instance *std* and set the ID, if this did not occur automatically during installation:

   ```
   . ftseti std; fta -s [-id=BEECH.FOREST.NET]
   ```

6. Next, make a shell script for administering the instance that handles the events *start*, *stop,* and *check*. The script must be available and properly configured on the computers **MAPLE** and **BEECH.** It might look like the following:

   ```
   PAR=$1
   BIN=/opt/bin; export BIN
   INST=cluster
   OPENFTINSTANCE=$INST; export OPENFTINSTANCE
   case $PAR in
   start) OPENFTINSTANCE=std; export OPENFTINSTANCE
      $BIN/ftcrei $INST /openFT/$INST
      case $? in
         0|5) continue;;
         *) exit 1;;
      esac
      OPENFTINSTANCE=$INST; export OPENFTINSTANCE
      $BIN/fta -s 2>/dev/null
      case $? in
         0|180) exit 0;;
         *) exit 1;;
      esac;;
   ```

```
stop) $BIN/fta -t 2>/dev/null
   case $? in
      0|181) continue;;
      *) exit 1;;
   esac
   OPENFTINSTANCE=std; export OPENFTINSTANCE
   $BIN/ftdeli cluster
   case $? in
      0) exit 0;;
      *) exit 1;;
   esac;;
check) VALUE=`$BIN/fti -csv -p 2>/dev/null |fgrep FtStarted\
               |sed s/";"/" "/g`
   [ -z $VALUE ] && exit 1
   set $VALUE
   i=1
   FTROW=1
   while [ "$1" != "FtStarted" ]
   do shift
   FTROW=`expr $FTROW + 1`
   done
   FTSTART=`$BIN/fti -p -csv|fgrep -v FtStarted|cut \
           -f$FTROW -d\;`
   if [ $FTSTART = '*NO'  ]
   then # fta not active
   exit 1
   else # fta active
   exit 0
   fi
   # # For using  openFT-FTAM activate the commands by
   # # removing the first "#"
   # FTAMROW=1
   # while [ "$1" != "FtamStarted" ]
   # do shift
   # FTAMROW=`expr $FTAMROW + 1`
   # done
   # FTAMSTART=`$BIN/fti -p -csv|fgrep -v FtamStarted \
   # |cut -f$FTAMROW -d\;`
   # if [ $FTAMSTART = '*NO'  ]
   # then # fta not active
   #       exit 1
   #else # fta active
   #    exit 0
   # fi
   ;;
esac
```

Working with individual instances

When everything is finished, there is a standard instance on both the MAPLE and BEECH computers which is not fail-safe. By making a selection on the graphical user interface, or by executing the command *ftseti std,* you will be working with the respective standard instance. You can make use of all the *open*FT functions in the standard instances (e.g. set up admissions profiles, view log records, etc.). The standard instances on MAPLE and BEECH can be addressed normally from external systems using the addresses of these computers (123.25.10.1 or 123.25.10.2).

The fail-safe instance *cluster* is available on one of these two computers; the one on which the disk */openFT* is currently mounted. You can work with the instance on this computer using the graphical user interface or by using the command *. ftseti cluster* and use all of *open*FT functions available there. It is not necessary to know on which computer the disk */openFT* is mounted during this. You must choose TREE as the partner. The UNIX cluster TREE (*open*FT instance *cluster*) is addressed externally under the IP address 123.25.10.12.

Example 2: Fail-safe capability for both computers in the cluster

The UNIX cluster, once again, consists of two computers: MAPLE (IP address 123.25.10.1) and BEECH (IP address 123.25.10.2).

In this example, however, there is to be a fail-safe *open*FT instance available on each of the two computers. For this purpose, the computers are superimposed (MAPLE by CL_MAPLE (IP address 123.25.10.10) and BEECH by CL_BEECH (IP address 123.25.10.20). If the computer MAPLE fails, then CL_MAPLE is switched over to the computer BEECH. If the computer BEECH fails, then CL_BEECH is switched over to the computer MAPLE.

Configure the UNIX cluster so that a disk is always available for each computer, for example: */sha_MAPLE* and */sha_BEECH*.

Required steps for the computer MAPLE

1. Configure a standard instance as shown in example 1.
2. Mount the disk */sha_MAPLE* and */sha_BEECH* on MAPLE.
3. Create and check the instances *MAPLE* and *BEECH*:

```
ftcrei MAPLE /sha_MAPLE/oFT –addr=CL_MAPLE.FOREST.NET
ftcrei BEECH /sha_BEECH/oFT –addr=CL_BEECH.FOREST.NET
ftshwi @a –l
```

4. Deactivate the instances *MAPLE* and *BEECH*:

```
ftdeli MAPLE
ftdeli BEECH
```

Required steps on the computer BEECH

1. Configure a standard instance as shown in example 1.
2. Next, make a shell script for controlling openFT on the computers MAPLE and BEECH that handles the events *start, stop, and check*. Both scripts must be available on both computers. The shell script might look like the example below (in the script for BEECH, the name *MAPLE* must be substituted with *BEECH* in the following):

```
PAR=$1
BIN=/opt/bin; export BIN
INST=MAPLE
OPENFTINSTANCE=$INST; export OPENFTINSTANCE
```

```
case $PAR in
start) OPENFTINSTANCE=std; export OPENFTINSTANCE
   $BIN/ftcrei $INST /sha_MAPLE/oFT
   case $? in
      0|5) continue;;
      *) exit 1;;
   esac
   OPENFTINSTANCE=$INST; export OPENFTINSTANCE
   $BIN/fta -s 2>/dev/null
   case $? in
      0|180) exit 0;;
      *) exit 1;;
   esac;;
stop) $BIN/fta -t 2>/dev/null
   case $? in
      0|181) exit 0;;
      *) exit 1;;
   esac
   OPENFTINSTANCE=std; export OPENFTINSTANCE
   $BIN/ftdeli $INST
   case $? in
      0)exit 0;;
      1)exit1;;
   esac;;
check) VALUE=`$BIN/fti -csv -p |fgrep FtStarted \
               |sed s/";"/" "/g`
   set $VALUE
   i=1
   FTROW=1
   while [ "$1" != "FtStarted" ]
   do shift
      FTROW=`expr $FTROW + 1`
   done
   FTSTART=`$BIN/fti -p -csv|fgrep -v FtStarted \
            |cut -f$FTROW -d\;`
   if [ $FTSTART = '*NO' ]
   then # fta not active
      exit 1
   else # fta active
      exit 0
   fi;;
esac
```

Working with the individual instances

When everything is finished, there is a standard instance on both the MAPLE and BEECH computers which is not fail-safe. By making a selection on the graphical user interface, or by executing the command *ftseti std,* you will be working with the respective standard instance. You can make use of all the *open*FT functions in the standard instances (e.g. set up admissions profiles, view log records, etc.). The standard instances on MAPLE and BEECH can be addressed normally from external systems using the addresses of these computers (123.25.10.1 or 123.25.10.2).

The *open*FT instances *MAPLE* and *BEECH* are available on the computer, on which the corresponding disk is currently mounted. They can be used, as usual, via the graphical user interface or the command interface. Another possibility exists using remote administration (where the partner is CL_MAPLE or CL_BEECH).

In order to transfer files to these instances, the IP addresses of CL_MAPLE.FOREST.NET or CL_BEECH.FOREST.NET (123.25.10.10 or 123.25.10.20) can be addressed.

Glossary

Cross-references are written in *italics*.

absolute Path name

The entire path name, from the root directory to the file itself.

access control

File attribute in the *virtual filestore*, attribute of the *security group*, that defines *access rights*.

Access Control List (ACL)

Mechanism for refining access control for shared disk files through to the level of individual users or named groups of users.

access protection

Comprises all the methods used to protect a data processing system against unauthorized system access.

access right

Derived from the *transfer admission*. It defines the scope of access for the user who specifies the transfer admission.

action list

Component of the file attribute *access control* in the virtual filestore that defines access rights.

admission set

FTAC uses the admission set to define for a particular login name the *partner systems* it is allowed to cooperate with and the FT functions it is allowed to use.

admission set, privileged

see privileged admission set

Advanced Encryption Standard (AES)

International standards for encrypting data to increase security. The AES method meets the latest encryption technique standards for 128 bit keys. The AES method is used by the FT products of the Fujitsu Siemens Computers GmbH to encrypt request description data and, possibly, for the request data.

ANSI code

Standardized 8-bit character code for message exchange. The acronym stands for "American National Standards Institute".

Application Entity Title (AET)

The Application Entity Title consists of Layer 7 addressing information of the *OSI Reference Model*. It is only significant for *FTAM partners*.

asynchronous request

The *FT request* is executed independently after the user has submitted the request. The user can continue his or her work once the system has confirmed acceptance of the request.

authentication

Process used by *open*FT to check the identity of the request partner.

background process

A process that runs independently of the user process. A background process is started by placing the special character & at the end of a command. The process which initiates the background process is then immediately free for further tasks and is no longer concerned with the background process, which runs simultaneously

basic functions

Most important file transfer functions. Several basic functions are defined in the *admission set* which can be used by a login name. The six basic functions are:

– inbound receive
– inbound send
– inbound follow-up processing
– inbound file management
– outbound receive
– outbound send

character repertoire

Character repertoire of a file in the *virtual filestore*.

cluster controller

Device for the connection between a transmission line and several terminals (data terminal).

communication controller

Data communication processor

compress

several consecutive identical characters are abbreviated to one character together with the number of the characters originally present. This reduces transfer times.

computer network, open

see *open computer network*

concurrency control

Component of the file attribute *access control* in the virtual filestore that controls concurrent access.

connectivity

In general, the ability of systems and partners to communicate with one another. Sometimes refers simply to the communication possibilities between transport systems.

constraint set

Component of the *document type*.

contents type

File attribute in the *virtual filestore*; attribute of the *kernel group* that describes the file structure and the form of the file contents.

CSV output format

This is a quasi-tabular output format that is very widely used in the PC environment in which the individual fields are separated by a semicolon ";". It permits the further processing of the output from the most important *open*FT commands using separate tools.

data communication system

Sum of the hardware and software which allows two or more communication partners to exchange data while adhering to specific rules.

data compression

Reducing the amount of data by means of compressed representation.

data encoding

Method of representing a character internally in an *FT system*.

Data Encryption Standard (DES)

International standardization of data to enhance data security. The DES procedure is used in the FT products of Siemens AG to encrypt the request description data and possibly the request data.

data protection

- In the narrow sense as laid down by law, the task of protecting personal data against misuse during processing in order to prevent the disclosure or misappropriation of personal information.
- In the wider sense, the task of protecting data throughout the various stages of processing in order to prevent the disclosure or misappropriation of information relating to oneself or third parties.

data security

Technical and organizational task responsible for guaranteeing the security of data stores and data processing sequences, intended in particular to ensure that

- only authorized personnel can access the data,
- no undesired or unauthorized processing of the data is performed,
- the data is not tampered with during processing,
- the data is reproducible.

DHCP

Service in TCP/IP networks that automatically assigns IP addresses and TCP/IP parameters to clients on request.

directory

In the tree structure of the UNIX file system or in BS2000 (POSIX), directories are lists that reference other files or directories.

In BS2000 (DVS), PLAM libraries are interpreted as directories.

document type

Value of the file attribute *contents type*. Describes the form of the file contents in the *virtual filestore*:
– document type for text files: FTAM-1
– document type for binary files: FTAM-3

EBCDIC

Standardized code for message exchange as used in BS2000/OSD. The acronym stands for "Extended Binary Coded Decimal Interchange Code".

emulation

Components that mimic the properties of another device.

entity

Term taken from the OSI architecture: active element in a layer.

Explorer

A program from Microsoft that is supplied with the Windows 95/98 and Windows NT operating systems to facilitate navigation within the file system.

file management

Option to manage files in the remote system.

The following options are available:
– Create directories
– Display and modify directories
– Delete directories (only via the program interface)
– Display and modify file attributes
– Rename files
– Delete files

Filestore, virtual

see *virtual filestore*

file transfer

File transfer

file transfer request

FT request

firewall processor

Processor which connects two networks. The possible access can be controlled precisely and also logged.

fixed-length record

A record in a file all of whose records possess the same, agreed length. It is not necessary to indicate this length within the file.

FJAM-LU

FT-specific software module required to connect *open*FT for OS/390 and z/OS to a *TRANSDATA network* via *TRANSIT-SNA*. FJAM-LU is part of TRANSIT-SNA.

follow-up processing

FT function that initiates execution user specific commands or statements in the *local* and/or *remote system* after an *FT request* has been completed. Different follow-up processing may be defined for positive and negative completion.

follow-up processing request

Statement contained within an *FT request* to effect *follow-up processing* after file transfer.

front-end processor

Connected to the I/O channel of the preprocessor. It connects the rest of the network to the preprocessor and serves the terminals connected to it.

FT administrator

Person who administers the FT product installed on a computer. *open*FT can be administered from the login names *root* and *admin*.

FT profile

Means of defining the protection functions of *FTAC*. FT profiles define a *transfer admission* that must be specified in *FT requests* in place of the *LOGIN authorization*. The FT profile defines the *access rights* of a particular login name by restricting the use of specific parameters in *FT requests*.

FT profile, privileged

see privileged FT profile

FT request

Request to an *FT system* to transfer a file from a *send system* to a *receive system* and possible start *follow-up processing requests*.

FT system

System for transferring file that consists of a computer and the software required for file transfer.

FT trace

Diagnostic function that logs FT operation.

FTAC (File Transfer Access Controll)

Part of *open*FT that offers extended access protection for file transfer and file management.

FTAC administrator

Administrator of the FTAC functions; should be identical to the person responsible for data security in the UNIX system.

FTAC logging function

Function which FTAC uses to log each access to the protected system via file transfer.

FTAM-1

document type for text files

FTAM-3

document type for binary files

FTAM catalog

The FTAM catalog is used to extend the file attributes available in UNIX. It is only relevant for access using FTAM. For example, a file can be deleted using the UNIX command *rm,* even if the *permitted actions* parameter does not allow this.

FTAM file attributes

All systems which permit file transfer via FTAM protocols must make their files available to their partners using a standardized description (ISO 8571). To this end, the attributes of a file are mapped from the physical filestore to a *virtual filestore* and vice versa. This process distinguishes between three groups of file attributes:

– kernel group: describes the most important file attributes.
– storage group: contains the file's storage attributes.
– security group: defines security attributes for file and system access control.

FTAM partner

Partner system which uses the *FTAM protocols* for communication.

FTAM protocol

Protocol for file transfer standardized by the International Organization for Standardization (ISO) (ISO 8571, FTAM).
FTAM stands for **F**ile **T**ransfer, **A**ccess and **M**anagement.

FTIF (File Transfer Interconnect Facility)

Has the task of interconnecting different transport systems for file transfer; implemented in *open*FTIF for UNIX or Windows.

FTIF gateway

Computer on which *open*FTIF is installed.

FTIF name

Name used by *open*FTIF for UNIX to identify the partner application in the destination system. This name is specified as a symbolic name (also referred to as GLOBAL NAME) for the partner application in a TNS entry in the FTIF processor.

functional Standard

Recommendation defining the conditions and the forms of application for specific ISO standards. The transfer of unstructured files is defined in the Europe and prestandard ENV 41 204; file management in the European prestandard CEN/CENELEC ENV 41205.

Gateway

Generally understood to mean a computer that connects two or more networks and which does not function as a bridge. Variants: gateway at network level (=router or OSI relay), transport and application gateway.

gateway processor

Communication computer that links a computer network to another *computer network*. The mapping of the different protocols of the various computer networks takes place in gateway processors.

General String

Character repertoire for file files transferred to and from *FTAM partners*.

GraphicString

Character repertoire for files transferred to and from *FTAM partners*.

heterogeneous network

A network consisting of multiple subnetworks functioning on the basis of different technical principles.

homogenous network

A network constructed on the basis of a single technical principle.

HOSTS file

Network administration file that contains the Internet addresses, the processor names and the alias names of all accessible computers.

IA5String

Character repertoire for files transferred to and from *FTAM partners*

inbound file management

Request issued in a *remote system* for which directories or file attributes of the *local system* can be displayed, file attribute modified or local file deleted.

inbound follow-up processing

Request issued in a *remote system* with *follow-up processing* in the *local system*.

inbound receive

Request issued in the *remote system*, for which a file is received in the *local system*.

inbound request

Request issued in a remote system, i.e. your FT system is the *remote system* for this request.

inbound send

Request issued in a *remote system* for which a file is sent from the *local system*.

Initiator

here: *FT system* in which an *FT request* was issued.

instance ID

The network-wide, unique address of an *open*FT instance.

interoperability

Ability of two *FT systems* to work together.

ISO/OSI Reference Model

The ISO/OSI Reference Model provides the framework for standardization of the communication in open systems.

job

Sequence of commands, statements and data.

job transfer

Transfer of a file that represents a j*ob* in the *receive system* and is initiated as such there.

kernel group

Group of file attributes of the *virtual filestore* that encompasses the kernel attributes of a file.

library

File with the internal structure (elements)

library elements

Part of the library. A library element can also be structured in records.

Local Area Network (LAN)

Originally a high-speed network with limited physical extension. Nowadays, any network, that uses CSMA/CD, Token Ring or FDDI irrespective of the range (see also *WAN Wide Area Network*).

local system

The *FT system* at which the user is working.

logging function

Function which *open*FT uses to log each access to the protected system via file transfer.

Logical Unit (LU)

Interface between an application program and the SNA data communications network. The LU type describes the communications characteristics.

log record

Contains information on an access check carried out by *open*FT.

LOGIN authorization

Transfer admission to a computer which (as a rule) consists of the login name and the password, and authorizes dialog operation, see also *LOGON authorization*.

LOGON authorization

Transfer admission to a computer which (as a rule) consists of the login name, the password and the account number, and authorizes dialog operation.

mailbox

The mailbox is a file which is read using the mail command. Each user has a mailbox for receiving messages.

maximum-string-length

Specifies the maximum string length of *strings* within a file in the *virtual filestore*.

NCP (Network Control Processor)

– Front-end-processor for SNA hosts

– Software that runs on an IBM data communications computer.

network description file

File that contains the data on the *remote systems* (*FT systems*).

open computer network

Computer network in which communication is carried out according to ISO rules. Interoperability of different computer from various manufacturers is possible using specified *protocols*.

***open*FTIF**

*open*FTIF performs the task of interconnecting different transport systems.

***open*FT instance**

Several *open*FT systems can simultaneously run *open*FT instances on a cluster in the TCP/IP network. Each instance has its own address (instance ID) and consists of the loaded code of the *open*FT products (including additional products if they are available) and of the variable files such as the log files, request log, etc.

***open*FT partners**

Partner systems which communicate via *open*FT *protocols*.

***open*FT protocols**

Protocols for file transfer standardized by Siemens (SN77309, SN77312).

***open*FT-FTAM (BS2000)**

Add-on product for *open*FT (BS2000) to support file transfer with *FTAM protocols*. FT-FTAM stands for File Transfer FTAM support.

***open*FT-FTAM for BS2000**

Add-on product for *open*FT for BS2000 to support file transfer with *FTAM protocols*. FT-OS stands for File Transfer OSI Support.

_open_FT-FTAM for UNIX

Add-on product for _open_FT for UNIX to support file transfer with _FTAM protocols_. Also includes OSI Layers 5 and 6 (protocol engine).

operating parameters

Parameters which control the _resources_ (e.g. possible number of connections)

outbound request

Request issued in own processor, i.e. the own FT system is the _local system_ for this request.

outbound receive

Request issued locally for which a file is received in the _local system_.

outbound send

Request issued locally for which a file is sent from the _local system_.

owner of an FT request

Login name in the _local system_ or _remote system_ under which this _FT request_ is executed. The owner is always the ID under which the request is submitted, not the ID under which it is executed.

partner system

here: _FT system_ that executes FT request together with the _local system_.

password

Sequence of characters that a user must enter in order to access a user ID, file, job variable, network node or application. The user ID password serves for user _authentication_. It is used for access control. The file password is used to check access rights when users access a file (or job variable). It is used for file protection purposes.

PDN

Communication computer control program, consisting of the computer's operating system and system programs for the handling of communications protocols.

permitted actions

File attribute in the *virtual filestore*; attribute of the *kernel group* that defines actions that are permitted in principle.

Physical Unit

In SNA this is an element that represents a device and may contain one or more *Logical Units*.

port number

Number that uniquely identifies a TCP/IP application or the end point of a TCP/IP connection within a processor.

POSIX (Portable Open System Interface)

Board and standards laid down by it for interfaces that can be ported to different system platforms.

postprocessing; file transfer with postprocessing

*open*FT makes it possible to process the received data in the receiving system through a series of operating system commands, under the process control of *open*FT (in contrast to *follow-up processing*).

preprocessing; jfile transfer with preprocessing

The preprocessing facility in *open*FT can be used to send a receive request in which the outputs of a remote command are transferred instead of a file. This makes it possible to query a database on a remote system, for example. Preprocessing also may be issued locally.

presentation

Entity that implements the Presentation Layer (Layer 6) of the *ISO Reference Model* in an *FT system* that uses *FTAM protocols*.

presentation selector

Subaddress used to address a *presentation application*

privileged FT profile

FT profile which the FTAC user may use to exceed the limits specified by the *FTAC administrator* in the *admission set*. To do this he or she requires permission from the FTAC administrator, who is the only person capable of assigning privileges.

privileged admission set

Admission set of the *FTAC administrators*. Exactly one admission set in the system has a privilege.

processor node

Entity in the host or communications computer that can be addressed throughout the network and that performs service functions for the exchange of data.

profile

In OSI, a profile is a standard which defines which protocols may be used for any given purpose and specifies the required values of parameters and options.

Here: a set of commands assigned to a user ID. The permissibility of these commands is ensured by means of syntax files. See also *admission profile*, *privileged admission profile*, *FTAC* profile.

prompting in procedures

Function used to prompt the user at the terminal to enter data required to run the procedure.

protocol

Set of rules governing information exchange between peer partners in order to achieve a defined objective. This usually consists of a definition of the messages that are to be exchanged and the correct sequencing of messages including the handling of errors and other exceptions.

public key

Published encryption key. It is defined and published by the recipient of a message or is communicated to the sender of the message to permit the encryption of the messages transmitted to the recipient. It is used by a variety of encryption procedures, including the *RSA* procedure. It must match the *secret key* that is known only to the recipient.

RAS

Remote Access Service; a Windows NT service that enables communication with remote systems.

receive file

File in the *receiving system*, in which the data from the *send file* are stored.

receive system

System to which a file is sent. This may be the *local system* or the *remote system*.

record

Set of data that is treated as a single logical unit.

relative path name

The path from the current *directory* to the file.

remote system

see *Partner system*

request

here: *FT request*

request ID

ID number of an *FT request*.

request management

FT function responsible for managing *FT request*; it ensures request processing from the submission of a request until its complete processing or termination.

request number

see *Request ID*

request queue

File which contains the *asynchronous requests* and their processing states. The request queue also contains the parameters set with the *fta* command.

request storage

FT function for storing *FT requests* until they have been completely processed or until they are terminated .

responder

here *FT system* addressed by the *initiator*.

resources

Hardware and software objects required by the *FT system* to execute an *FT request* (processes, connections, lines). These resources are controlled by the *Operating parameters*.

restart

Automatic continuation of an *FT request* after an interruption.

restart point

Point up to which data for the *send file* are stored in the *receive file* in the event of an interruption in file transfer and from which data are transferred after *restart*.

result list

List containing information about completed file transfer which the user receives in the *local system* for *FT request* submitted there.

RFC

Request for Comment; procedure used in the Internet for commenting on proposed standards, definitions or reports; also used to denote a document agreed in this way.

RFC1006

RFC standard for an ISO transport service via TCP

router

Network element that is located between networks and guides message flows through the networks while simultaneously performing route selection, addressing and other functions. Operates on layer 3 of the OSI model.

secret key

Secret decryption key used by the recipient to decrypt a message that was encrypted using a *public key*. Used by a variety of encryption procedures including the *RSA procedure*.

security attributes

An object's security attributes specify how and in what ways the object may be accessed.

security group

Group of file attributes in the *virtual filestore*, encompassing the security attributes of a file.

security level

When using *FTAC functions*, the security level is a measure of the security requirement with respect to the *partner system*.

send file

File in the *sending system* from which data is transferred to the *receive file*.

sending system

here: *FT system* that sends a file. This may be the *local system* or the *remote system*.

service

As used in the OSI architecture: a service is the set of functions that a service provider makes available at a service access point.

As used in the client/server architecture: a set of functions that a server makes available to its clients.

service class

Parameter used by *FTAM partners* to negotiate the functions to be used.

session

In OSI, the term used for a layer 5 connection.

In SNA, a general term for a connection between communication partners (applications, devices or users).

session selector

Subaddress used to address a *session application.*

shell metacharacters

The following metacharacters have special meanings for the shell:

*, [ ], ?, <, >, |, &, &&, ( ), { }

SNA network

Data communication system that implements the Systems Network Architecture (SNA) of IBM.

SNMP (Simple Network Management Protocol)

Protocol for TCP/IP networks defined by the IP (Internet Community) for the transfer of management information.

special characters

see *shell metacharacters.*

standard error output (stderr)

By default, standard error output is to the screen.

standard input (stdin)

By default, standard input is from the keyboard.

standard output (stdout)

By default, standard output is to the screen.

storage group

Group of file attributes of the *virtual filestore*, encompasses the storage attributes of a file.

string

A character string

string significance

Describes the format of *strings* in files to be transferred using FTAM protocols.

synchronous request

The user process that submitted the *FT request* waits until the transfer has been completed

system

see *FT system*

system, remote

see *remote system*

system, local

see *local system*

TCP/IP (Transmission Control Protocol/Internet Protocol)

Widespread protocol for file transfer (corresponds roughly to Layers 3 and 4 of the OSI Reference Model, i.e. Network and Transport Layer); was originally developed for the ARPANET (computer network of the US Ministry of Defense, now a de-facto standard.

TRANSDATA network

Data communication system that implements the TRANSDATA network concept. Products used to connect TRANSDATA networks to *SNA networks* include, for example, *TRANSIT-CD* and *TRANSIT-SNA*.

transfer admission

Authorization to access a particular login name. With *open*FT, specific transfer admissions may be defined for file transfer to replace the *LOGIN authorizations*.

transfer identification

see *request identification.*

TRANSIT-CD

Product of Fujitsu Siemens Computers used to link *TRANSDATA networks* and *SNA networks*.

TRANSIT-Server andTRANSIT-CLIENT

Product of Fujitsu Siemens Computers used to link Reliant UNIX systems and *SNA networks*.

TRANSIT-SNA

Product of Fujitsu Siemens Computers used to link *TRANSDATA networks* and *SNA networks*.

Transmission Control Protocol/Internet Protocol

see *TCP/IP*

transport connection

Logical connection between two users of the transport system (terminals or applications).

Transport Name Service (TNS)

Service used to administer properties specific to transport systems. Entries for *partner systems* receive the information on the particular *transport system* employed.

transport protocol

Protocol of the *Transport Layer*

Transport Layer

Layer 4 of the *OSI Reference Model*. The Transport Layer handles the protocols for the transport of data.

transport selector (T selector)

Subaddress used to access an application in the *Transport Layer*.

transport system

- The part of a system or architecture that performs approximately the functions of the four lower OSI layers, i.e. the transport of messages between the two partners in a communication connection.
- Sum of the hardware and software mechanisms that allow data to be transported in computer networks.

transfer unit

The smallest data unit used to transport data in FTAM transfer. For *FTAM-1* and *FTAM-3*, these are *strings*. A transfer unit can, but need not, correspond to a file record.

universal class number

Character repertoire of a file in the *virtual filestore*.

variable length record

A record in a file all of whose records may be of different lengths. The record length must either be specified in a record length field at the start of the record or must be implicitly distinguishable from the next record through the use of a separator (e.g. Carriage Return -Line Feed).

virtual filestore

The virtual filestore is used by FT systems acting as *responders* to make their file available to their *partner systems*. The way a file is represented in the virtual filestore is defined in the FTAM standard, see *file attributes*.

visibleString

Character repertoire for files transferred to and from *FTAM partners*.

Wide Area Network(WAN)

A public or private network that can span large distances but which runs relatively slowly and with higher error rates when compared to a *LAN*. Nowadays, however, these definitions have only limited validity.
Example: in ATM networks.

X terminal

A terminal or software component to display the graphical X Window interface of UNIX. An X terminal or a corresponding software emulation is a prerequisite for using the graphical interface of *open*FT.

Abbreviations

ACSE
Association Control Service Element

AES
Advanced Encryption Standard

AET
Application Entity Title

ANSI
American National Standards Institute

ASCII
American Standard Code for Information Interchange

BCAM
Basic Communication Access Method

BSFT
Byte Stream File Transfer

CAE
Common Application Environment

CEN
Comite Europeen de Normalisation

CENELEC
Comite Europeen de Normalisation Electrotechnique

CMX
Communication Manager SINIX

CCP
Communication Control Programm

DCAM
Data Communication Access Method

DCM
Data Communication Method

DES
Data Encryption Standard

DIN
Deutsches Institut für Normung (German standards institute)

DNS
Domain Name Service

EBCDIC
Extended Binary-Coded Decimal Interchange Code

ENV
Europäischer Normen-Vorschlag (European prestandard)

FADU
File Access Data Unit

FJAM
File Job Access Method

FSB
Forwarding Support Information Base

FSS
Forwarding Support Service

FT
File Transfer

FTAC
File Transfer Access Control

FTAM
File Transfer, Access and Management (ISO 8571)

FTIF
File Transfer Interconnect Facility

GPL
Gnu Public Licencse

GSM
Global System for Mobile Communication

ISAM
Index Sequential Access Method

ISO
International Organization for Standardization

LAN
Local Area Network

LMS
Library Maintenance System

MSV
Mittelschnelles Synchron Verfahren (Medium-fast synchronous method)

NDMS
Network Data Management System

NIS
Network Information Service

OSI
Open Systems Interconnection

OSS
OSI Session Service

PAM
Primary Access Method

PDN
Program system for data transmission and access control

PICS
Protocol Implementation Conformance Statement

PLAM
Primary Library Access Method

RFC1006
Request for Comments 1006

SAM
Sequential Access Method

SDF
System Dialog Facility

SNA
Systems Network Architecture

SNPA
Subnetwork Point of Attachment

TCP/IP
Transmission Control Protocol/Internet Protocol

TID
Transport Identification

TNSX
Transport Name Service in SINIX

TPI
Transport Protokoll Identifier

TS
Transport System

WAN
Wide Area Network

Related publications

The manuals are available as online manuals, see *http://manuals.fujitsu-siemens.com*, or in printed form which must be payed and ordered separately at *http://FSC-manualshop.com*.

***open*FT for UNIX**
Enterprise File Transfer in the Open World
User Guide

***open*FT for Windows**
Enterprise File Transfer in the Open World
User Guide
(only online available)

***open*FT for BS2000/OSD**
Enterprise File Transfer in the Open World
User Guide

***open*FT for BS2000/OSD**
Installation and Administration
System Administrator Guide

***open*FT for BS2000/OSD**
Program Interface
Programming Manual

***open*FTIF for UNIX**
File Transfer Interconnect Facility with UNIX
User Guide

***open*FT for OS/390 and z/OS**
Enterprise File Transfer in the Open World
User Guide

***open*FT for OS/390 and z/OS**
Installation and Administration
System Administrator Guide

CMX
Operation and Administration
User Guide

CMX
Programming Applications
Programming Manual

OSS(SINIX)
OSI Session Service
User's Guide

X/Open CAE Specification
Byte Stream File Transfer (BSFT)
X/Open Document Number XO/CAE/91/400
X/OPEN Company Limited
November 1991

Index

$FJAM 46, 49
$FJAM_OUTBOUND 46
$FJAM0nn 49
$FTAM 47

A
access rights
  transferred file 20
actions, system-wide 79
administer *open*FT
  fta command 85
administrator privileges
  assign 110
admission set
  backup 18
  CSV output format 130
  modify 110
AES/RSA 20, 38
AET 178
Application Entity Title 178
asynchronous requests
  deleting 92
  *open*FT not started 10
automatic installation 43

B
block length 87
  station link 9
BS2000 not accessible 151

C
change
  key 86
  order of requests 122
changing the default language setting
  ftlang command 109
checklist for FTAM 60
cluster 22
cluster configuration
  TNS entries 45
cluster switching 22
  SNMP 41
CMX 31
CMX commands 165
code table
  EBCDIC.DF.04 163
  ISO 8859-1 164
command 81
  ftalarm 92
  tnsxcom 166
  tnsxprop 167
command syntax 80
commands
  long 82
configuration 31
conslog 21
console commands
  message file for 21
controlling
  diagnostics (SNMP) 76
conversion table
  EBCDIC to ISO8859 161
  ISO8859 to EBCDIC 162
correction version
  install 37
create
  TS directory 166
create-new-key 76
creating an FT profile
  ftcrep command 95
creating an instance 22
creating or activating an instance
  ftcrei command 93
cref 159
CSV format, ftshwe 83
CSV output format
  admission set 130
  FT profile 146
  general description 83
CSV output format of FT profiles and
  admission sets from a file 134

D
data security 8
date 80
deactivating 23
deactivating an instance 23
definition of
local TS application 49
local TS application (FTAM) 52
remote TS application 53
remote TS application (FTAM) 59
delete
FT profile 17
FT profiles 102
log record 100
log record (automatic) 41
deleting
asynchronous requests 92
deleting an instance
ftdeli command 99
deleting FT profiles
ftdelp command 102
deleting log records
ftdell command 100
deleting requests unconditionally
ftrs command 125
DES/RSA 20, 38
diagnostic information
display 131
diagnostics (SNMP) 73
control 76
directories
create 98, 115, 121
delete 98, 115, 121
display 98, 115, 121
rename 98, 115, 121
display
admission set 127
FT profiles 142
log records 135
displaying diagnostic information
ftshwd command 131
displaying FT profiles and admission sets
ftshwe command 133

E
EMANATE 71
encryption
change with fta 86
of user data 38
software for 38
ending
*open*FT 10
entering TS applications 44
for partner system 53
entries for follow-up processing 82
entries in the command sequence 82
error diagnosis 21, 155
exiting
*open*FT 85
export
FT profile 104
export environment 104
exporting FT profiles and admission sets
ftexpe command 104
exporting the FTAC environment 104

F
file
standard response 43
file attributes
display 98, 115, 121
modify 98, 115, 121
file name 80
file transfer
with preprocessing 190
file type 94, 116
files
delete 98, 115, 121
rename 98, 115, 121
firewall 45
follow-up processing
entries 82
front-end processor 180
FT log record
delete 100

FT profile
CSV output format 146
export 104
modify 117
privilege 117
read from file 106
saving 18
write in a file 104
FT profiles
delete 102
display 142
FT profiles and admission sets from a file
CSV output format 134
fta 85
fta processes 86
FTAC administrator 8
identify 129
FTAC environment
exporting 104
importing 106
FTAC log 89
ftalarm command 92
enable automatically 41
FTAM 43
FTAM partner
entering 59
FTAM-1, FTAM-3 181
ftc 79, 92
ftcrei command
messages 94
ftcrep 79
ftdeli 99
ftdeli command
messages 99
ftdell 100
ftdelp 79, 102
ftDiagStatus 76
ftEncryptKey 76
ftexpe 104
ftexpe example 105
fthelp 13
fti 79
ftimpe 106
ftimpe example 107
ftlang 109
ftmoda 79, 110
ftmodi 116
ftmodi command
messages 116
ftmodp 79
ftmodr 79, 122
ftrs 125
ftshwa 127
example 128
ftshwd 131
ftshwe
CSV format 83
ftshwl 13, 79, 135
output 141
ftshwp 79, 142
ftStartandStop 74
ftStatActive 75
ftStatFinished 75
ftStatLocalReqs 75
ftStatLocked 75
ftStatRemoteReqs 75
ftStatWait 75
ftstd 47, 54
ftstdisdn 47, 55
ftSysparCode 74
ftSysparMaxInboundRequests 74
ftSysparMaxISP 74
ftSysparMaxLifeTime 74
ftSysparMaxOSP 74
ftSysparProcessorName 74
ftSysparStationName 74
ftSysparTransportUnitSize 74
ftSysparVersion 74
fttrace 21, 156, 158
ftupdi 148
ftupdk 149
full installation 31, 33

G

GLOBAL NAME 44

I
ignore entries of administrator 98, 121
importing admission sets
ftimpe command 106
importing FT profiles
ftimpe command 106
importing FT profiles and admission sets 106
importing the FTAC environment
ftimpe command 106
INBOUND-FILE-MANAGEMENT 128, 129
INBOUND-PROCESSING 128
INBOUND-RECEIVE 128
INBOUND-SEND 128
information
ion the Internet 6
on instances 23
initial installation 31, 33
installation 31
automatic 43
correction version 37
full 31, 33
initial 31, 33
of a patch 37
of *open*FT-FTAM 31
update 31
instance 22, 23
creating 22, 93
deleting 99
modifying 22, 116
query information on 23
setup 23
instance ID 25, 186
Internet
information 6
Internet-addresses
variable 56
intrusion attempts
prevent 15
ISDN 55

K
key
change with fta 86

L
local system
specify name 39
local TS application
defining 49
definition (FTAM) 52
log
FTAC 89
log file
corrupted 152
log IDs 141
log record
with postprocessing 141
with preprocessing 141
log records
automatic delete 41
delete 100
output 141
partner name missing 151
logging
default setting 89
selection 89
logging function
cannot be called 152
lose privileged status
FT profiles 106

M
MAX. ADM LEVELS 98, 121
MAXISP 9
maxisp 88
MAXISP / MAXOSP
recommendations 9
MAXOSP 9
maxosp 88
maxsdata 158
maxstypeddata 158
maxuserdata 157
message file for console
commands 21

messages of the ftcrei command 94
messages of the ftdeli command 99
messages of the ftmodi command 116
modification date 90
modify
admission set 110
FT profile 117
instance 22
modifying an instance
ftmodi command 116

N

name
symbolic 44, 53
ncopy
no free transport connection 152
NCP generation 66
new installation 31
new key 86
noev 157
non-execution
asynchronous requests 10
Notational conventions 6
notify
name of the local system 39
number
of simultaneous requests 9
NUMBER OF PROFILES 131
NUMBER OF UADS 131

O

*open*FT
automatic start 40
automatic terminate 40
ending 10
exiting 86
starting 10, 86
starting / stopping (SNMP) 73, 74
*open*FT commands 77
*open*FT instances 22
*open*FT subagent 71
starting 72
*open*FT-CR 32, 38
*open*FT-FTAM 42
*open*FTIF 57, 63
OUTBOUND-RECEIVE 128
OUTBOUND-SEND 128
output
log records 141
properties of TS applications 167
output in CSV format 83
ftshwa 129
ftshwp 146

P

partner name
partner 81
patch 37
PCMX 31
PDN 189
PDN generation 68
performance control 9
port number 50
*open*FT-FTAM 52
postprocessing
log record 141
preprocessing 190
log record 141
priority
requests 122
PRIV 129
priv 120
privilege, FT profile 17
privileged profile 120
processor name 88
profile name 81
protection bit setting 20
protective bit setting 86
public key encryption
SNMP 76
public key for encryption (SNMP) 73

Q

query
information on instances 23
query language 109

R
reason code
display 13
remote TS application
definition 53
definition (FTAM) 59
reporting failed requests
ftalarm command 92
request lifetime 89
request queue 192
administer 12
requests
simultaneous 9
root
admission set 15
RSA/AES 20, 38
RSA/DES 20, 38

S
saving
log records 13
standard admission set 18
security
measures 15
sequence
entries in the command 82
set
parameters 85
setting up an instance 23
simultaneous requests 85
number of 9
SNA link 49
SNMP 71
automatically starting
administration 41
cluster 72
cluster switching 41
diagnostics control 76
public key encrypting 76
special characters 82
specify name
of the local systems 39
SSID 131
standard admission set 14
not saved 106
recommendation 15
standard entry
for ISDN 55
for TCP/IP 54
standard response file 43
starting
automatic (*open*FT) 40
*open*FT 10, 85
statistical data (SNMP) 73
statistical information (SNMP) 75
status
of *open*FT (SNMP) 73
step 21, 156, 158
subagent for *open*FT 71
switching clusters 22
switching the language interface 11
symbolic name 44, 53
system parameters (SNMP) 74
system-wide actions 79

T
TCP/IP 54, 196
terminate
automatic (*open*FT) 40
TNS 44
TNS compiler 44
TNS entries
automatically created 45
cluster configuration 45
tnsxcom 44, 166
tnsxprop 167
trace 21, 86, 155
file names 155
trace files 155
evaluate 156, 158
FTAM partner systems 157
Trace mode 85
transfer admission 81
TRANSIT-CLIENT 196
TRANSIT-Server 196
Transport Name Service 44

transport system applications
entering 44
TS application
entering 44
output properties of 167
TS directory
create 166

U
umask 20
update installation 31
user data
encrypt 38
user id 80
using disabled basic functions 98, 121

V
variable Internet addresses 56

W
what if ... 151

X
X terminal 198

Contents

1 Preface 1
1.1 Brief description of the product 2

1.3 Concept of *open*FT for UNIX manuals 3
1.4 Changes since the last version of the manual 4
1.5 Notational conventions 6
1.6 README files 6
1.7 Current information on the Internet 6

2 Tasks of the administrator 7
2.1 Operating parameters 9
2.2 Starting and stopping *open*FT 10
2.3 Switching the language interface 11
2.4 Request queue 12
2.5 Log records 13
2.5.1 Displaying log records 13
2.5.2 Deleting log records 13
2.6 Admission sets 14
2.6.1 Standard admission set 14
2.6.2 Displaying and modifying admission sets 14
2.6.3 Using admission sets properly 15
2.7 FT profiles 16
2.7.1 Creating FT profiles 16
2.7.2 Viewing and modifying FT profiles 16
2.7.3 Deleting FT profiles 17
2.7.4 Assigning privileges to FT profiles 17
2.8 Saving the FTAC environment 18
2.8.1 Saving admission sets and FT profiles 18
2.8.2 Importing saved admission sets and FT profiles 19
2.9 Setting the protection bit for newly created files 20
2.10 AES encryption method 20
2.11 Diagnosis 21
2.12 Using *open*FT in a cluster 22
2.13 Authentication 25
2.13.1 Instance Identifications 25
2.13.2 Creating and administering local keys 27
2.13.3 Distributing the keys to partner systems 28
2.13.4 Administering the keys of partner systems 29
2.13.5 Local and partner authentication 29

3 Installation and configuration 31
3.1 Installation of *open*FT 31
3.1.1 Initial or full installation 33
3.1.2 Update installation from *open*FT V8.0 35
3.1.3 Installation of a patch 37
3.1.4 Activities after installation 38
3.1.5 Automatic installation 43
3.2 Entering transport system applications 44
3.2.1 TNS entries created automatically 45
3.2.2 Definition of local TS applications for *open*FT for SNA links . . 49
3.2.3 Definition of the local TS application for *open*FT-FTAM 52
3.2.4 Definition of a remote TS application for *open*FT 53
3.2.4.1 Sample entries for *open*FT partners 56
3.2.4.2 *open*FTIF example for UNIX-UNIX link via *open*FT protocol . . . 57
3.2.5 Definition of remote TS applications for *open*FT-FTAM 59
3.2.5.1 Sample entries for FTAM partners 62
3.2.5.2 *open*FTIF sample for UNIX-UNIX link via FTAM protocol 63
3.3 Linking *open*FT for UNIX to *open*FT for OS/390 and z/OS via an SNA network 65
3.3.1 Sample generation for the link TRANSIT 65
3.3.2 Sample generation for the link to *open*FT for OS/390 and z/OS via TRANSIT-CD without TRANSIT 67

4 Administering *open*FT via SNMP 71
4.1 Activities after installation 71
4.2 Starting the *open*FT subagent 72
4.3 SNMP management for *open*FT 73
4.3.1 Starting and stopping *open*FT 74
4.3.2 System parameters 74
4.3.3 Statistical information 75
4.3.4 Control of diagnostics 76
4.3.5 Public key for encryption 76

5 *open*FT commands for the administrator 77
5.1 Overview of the commands 78
5.2 Notational conventions 80
5.3 Output in CSV format 83
5.4 fta - Administer *open*FT 85
5.5 ftalarm - Report failed requests 92
5.6 ftcrei - Create or activate an instance 93
5.7 ftcrep - Create an FT profile 95
5.8 ftdeli - Delete or deactivate an instance 99
5.9 ftdell - Delete log record 100
5.10 ftdelp - Delete FT profiles 102

5.11 ftexpe - Export FT profiles and admission sets . . . 104
5.12 ftimpe - Import profiles and admission sets . . . 106
5.13 ftlang - Change default language setting . . . 109
5.14 ftmoda - Modify admission sets . . . 110
5.15 ftmodi - Modify an instance . . . 116
5.16 ftmodp - Modify FT profiles . . . 117
5.17 ftmodr - Change the order of requests in the request queue . . . 122
5.18 ftrs - Delete requests unconditionally . . . 125
5.19 ftshwa - Display admission sets . . . 127
5.19.1 CSV output format for an admission set . . . 130
5.20 ftshwd - Display diagnostic information . . . 131
5.21 ftshwe - Display FT profiles and admission sets from a file . . . 133
5.21.1 CSV output format of FT profiles and admission sets from a file 134
5.22 ftshwl - Display log records . . . 135
5.22.1 Description of log record output . . . 141
5.22.1.1 Logging requests with preprocessing/postprocessing . . . 141
5.23 ftshwp - Display FT profiles . . . 142
5.23.1 CSV output format for an FT profile . . . 146
5.24 ftupdi - Update the instance directory . . . 148
5.25 ftupdk - Update public keys . . . 149
5.26 install.ftam - Install *open*FT-FTAM . . . 150

6 What if 151
6.1 Actions in the event of an error . . . 154

7 Diagnosis . . . 155
7.1 Trace files . . . 155
7.1.1 Evaluating trace files for *open*FT partner systems . . . 156
7.1.2 Defining the range of trace files for FTAM partner systems . . . 157
7.1.3 Evaluating trace files for FTAM partner systems . . . 158
7.2 Code tables . . . 161
7.2.1 Code conversion table EBCDIC.DF.04-x to ISO8859-x . . . 161
7.2.2 Code conversion table ISO8859-x to EBCDIC.DF.04-x . . . 162
7.2.3 Code table EBCDIC.DF.04 . . . 163
7.2.4 Code table ISO 8859-1 . . . 164

8 Appendix . . . 165
8.1 Important CMX commands . . . 165
tnsxcom - Create the TS directory . . . 166
tnsxprop - Output properties of TS applications . . . 167

8.2 *open*FT in a UNIX Cluster 169
Software requirements 169
Example 1: a fail-safe instance 170
Example 2: Fail-safe capability for both computers in the cluster 174

Glossary 177

Abbreviations 199

Related publications 203

Index 205

*open*FT V8.1 for UNIX

Enterprise File Transfer in the Open World
Installation and Administration
System Adminstrator Guide

Target group
This manual is aimed at the administrator of *open*FT for UNIX.

Contents
The manual describes the installation and configuration of *open*FT for UNIX and contains the command interface to administer *open*FT for UNIX. Administering via SNMP ist also described.

Edition: January 2004

File: ftuni_sv.pdf

Copyright © Fujitsu Siemens Computers GmbH 2004.

All rights reserved.
Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

This manual was produced by
cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Fujitsu Siemens Computers GmbH
User Documentation
81730 Munich
Germany

Fax: (++49) 700 / 372 00000

e-mail: manuals@fujitsu-siemens.com
http://manuals.fujitsu-siemens.com

Comments
Suggestions
Corrections

Submitted by

Comments on *open*FT V8.1 for UNIX
Enterprise File Transfer in the Open World - Installation and Administration

Information on this document

On April 1, 2009, Fujitsu became the sole owner of Fujitsu Siemens Computers. This new subsidiary of Fujitsu has been renamed Fujitsu Technology Solutions.

This document from the document archive refers to a product version which was released a considerable time ago or which is no longer marketed.

Please note that all company references and copyrights in this document have been legally transferred to Fujitsu Technology Solutions.

Contact and support addresses will now be offered by Fujitsu Technology Solutions and have the format *...@ts.fujitsu.com*.

The Internet pages of Fujitsu Technology Solutions are available at *http://ts.fujitsu.com/*...
and the user documentation at *http://manuals.ts.fujitsu.com*.

Copyright Fujitsu Technology Solutions, 2009

Hinweise zum vorliegenden Dokument

Zum 1. April 2009 ist Fujitsu Siemens Computers in den alleinigen Besitz von Fujitsu übergegangen. Diese neue Tochtergesellschaft von Fujitsu trägt seitdem den Namen Fujitsu Technology Solutions.

Das vorliegende Dokument aus dem Dokumentenarchiv bezieht sich auf eine bereits vor längerer Zeit freigegebene oder nicht mehr im Vertrieb befindliche Produktversion.

Bitte beachten Sie, dass alle Firmenbezüge und Copyrights im vorliegenden Dokument rechtlich auf Fujitsu Technology Solutions übergegangen sind.

Kontakt- und Supportadressen werden nun von Fujitsu Technology Solutions angeboten und haben die Form *...@ts.fujitsu.com*.

Die Internetseiten von Fujitsu Technology Solutions finden Sie unter *http://de.ts.fujitsu.com/*..., und unter *http://manuals.ts.fujitsu.com* finden Sie die Benutzerdokumentation.

Copyright Fujitsu Technology Solutions, 2009